US007664701B2

(12) **United States Patent**
Phillips et al.

(10) **Patent No.:** **US 7,664,701 B2**
(45) **Date of Patent:** **Feb. 16, 2010**

(54) **MASKING PRIVATE BILLING DATA BY ASSIGNING OTHER BILLING DATA TO USE IN COMMERCE WITH BUSINESSES**

(76) Inventors: **Christopher Phillips**, 22612 NE. 142nd Pl., Woodinville, WA (US) 98072; **G. Eric Engstrom**, 12415 Holmes Point Dr. NE., Kirkland, WA (US) 98033

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 237 days.

(21) Appl. No.: **11/591,696**

(22) Filed: **Nov. 1, 2006**

(65) **Prior Publication Data**

US 2007/0106609 A1 May 10, 2007

Related U.S. Application Data

(62) Division of application No. 09/553,068, filed on Apr. 20, 2000.

(51) **Int. Cl.**
G06Q 40/00 (2006.01)

(52) **U.S. Cl.** **705/40**; 705/44; 705/38

(58) **Field of Classification Search** 705/39, 705/40, 35, 26, 44, 38
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,883,810	A	3/1999	Rosen et al.	
6,456,984	B1	9/2002	Demoff et al.	
6,636,833	B1	10/2003	Flitcroft et al.	
7,337,144	B1 *	2/2008	Blinn et al.	705/40
2001/0044787	A1	11/2001	Shwartz et al.	
2002/0120587	A1	8/2002	D'Agostino	
2003/0028481	A1	2/2003	Flitcroft et al.	
2004/0158532	A1	8/2004	Breck et al.	

FOREIGN PATENT DOCUMENTS

WO	WO 99/13421 A2	3/1999
WO	WO 99/49424 A1	9/1999
WO	WO 00/65517 A1	11/2000

OTHER PUBLICATIONS

PR Newswire article Citibank and First City BankCorporation of Texas in Merchant Credit Card Processing Agreement, Jul. 19, 1990.

* cited by examiner

Primary Examiner—Jagdish N Patel
(74) *Attorney, Agent, or Firm*—Schwabe, Williamson & Wyatt, P.C.

(57) **ABSTRACT**

A method and apparatus for shielding a user's private billing data, such as credit card information, or other billing arrangements, but distributing different billing data to businesses during commerce therewith. Also disclosed is assigning the different billing data through real-time and advance distribution of the different billing data to a user, as well. Also disclosed is validating the correctness of a charge through confirmation of the charge with a financial institution, such as a bank, and by comparing itemized charges against expected charges identified by the user.

18 Claims, 5 Drawing Sheets

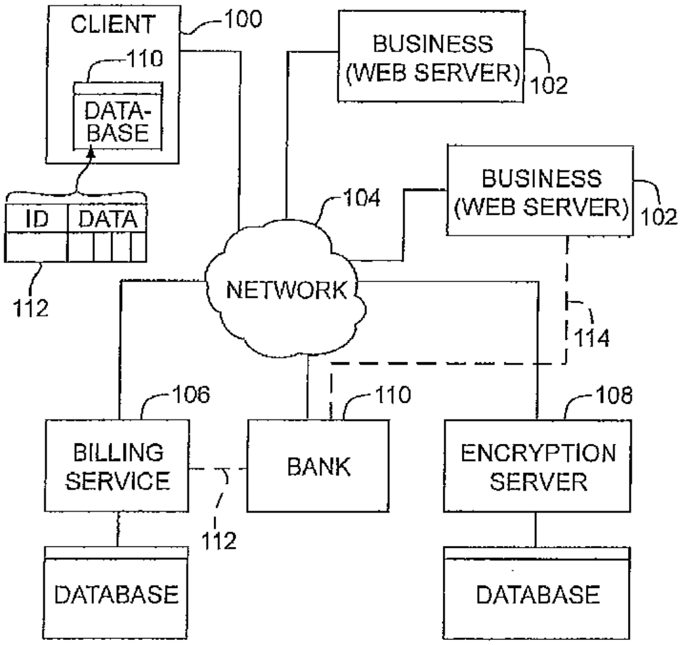
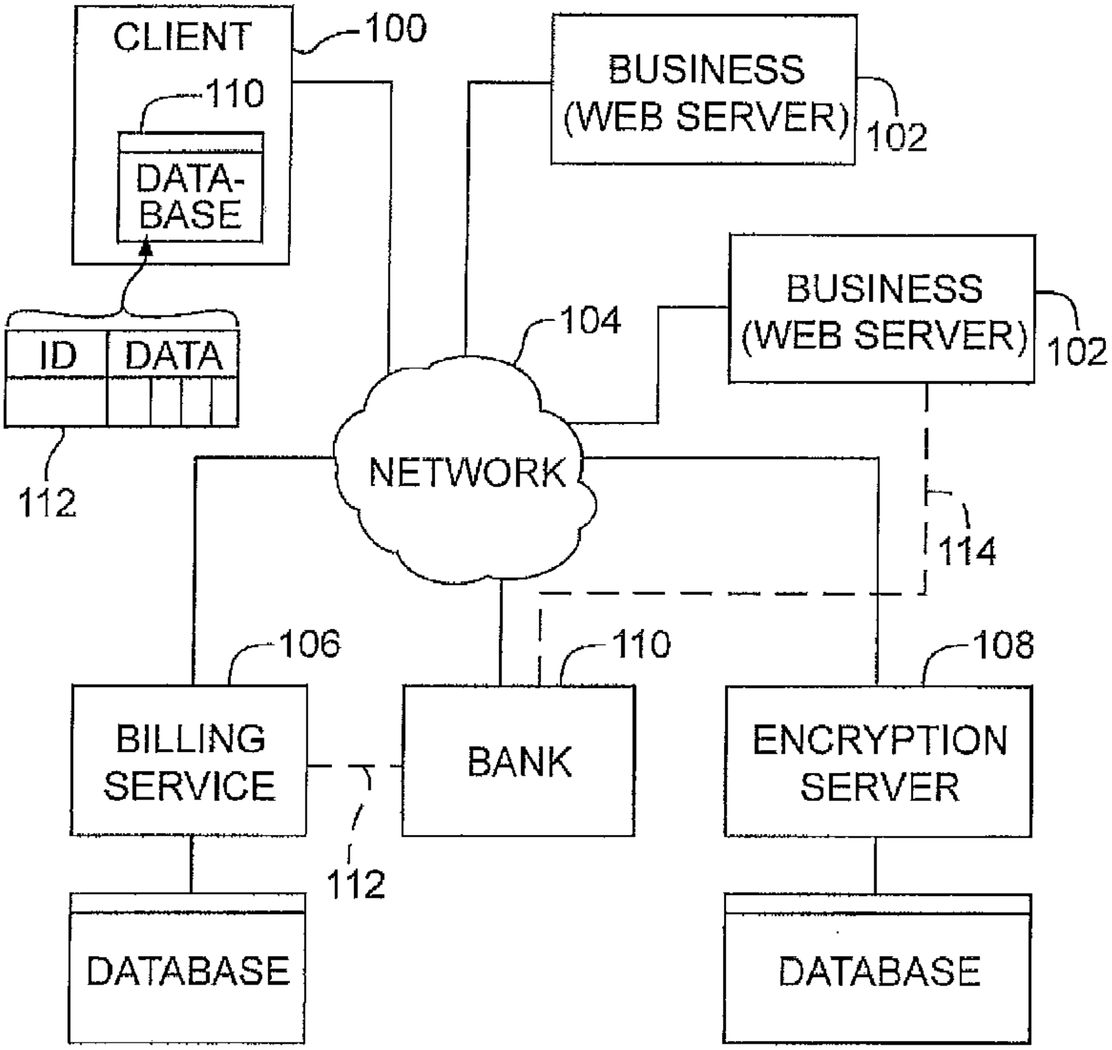


FIG. 1


CLIENT
100
110
DATA-BASE
ID
DATA
112
BUSINESS (WEB SERVER)
102
BUSINESS (WEB SERVER)
102
104
NETWORK
114
106
110
108
BILLING SERVICE
BANK
ENCRYPTION SERVER
112
DATABASE
DATABASE

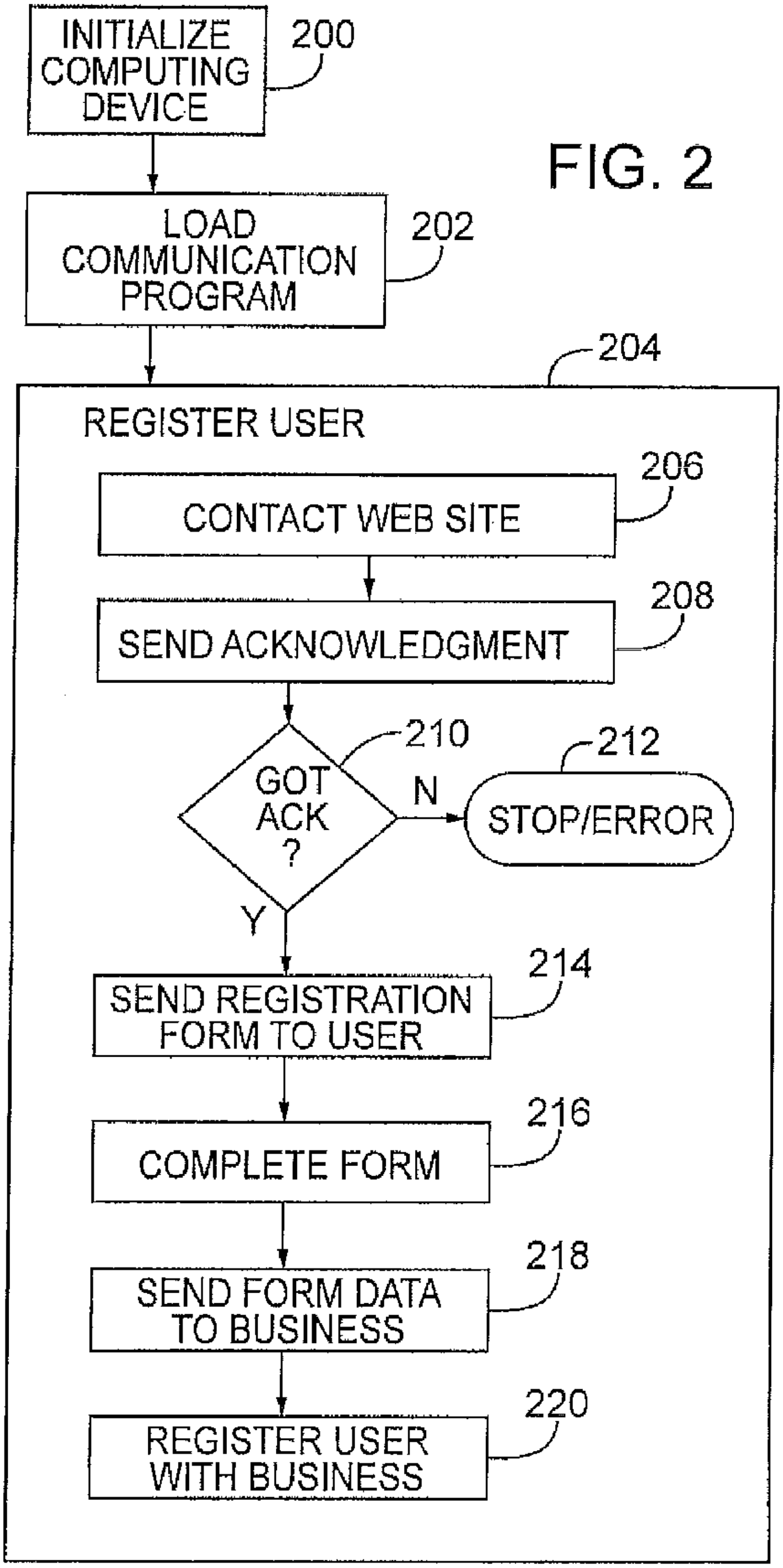

INITIALIZE COMPUTING DEVICE
200
LOAD COMMUNICATION PROGRAM
202
204
REGISTER USER
CONTACT WEB SITE
206
SEND ACKNOWLEDGMENT
208
GOT ACK ?
210
N
STOP/ERROR
212
Y
SEND REGISTRATION FORM TO USER
214
COMPLETE FORM
216
SEND FORM DATA TO BUSINESS
218
REGISTER USER WITH BUSINESS
220

FIG. 2

FIG. 3

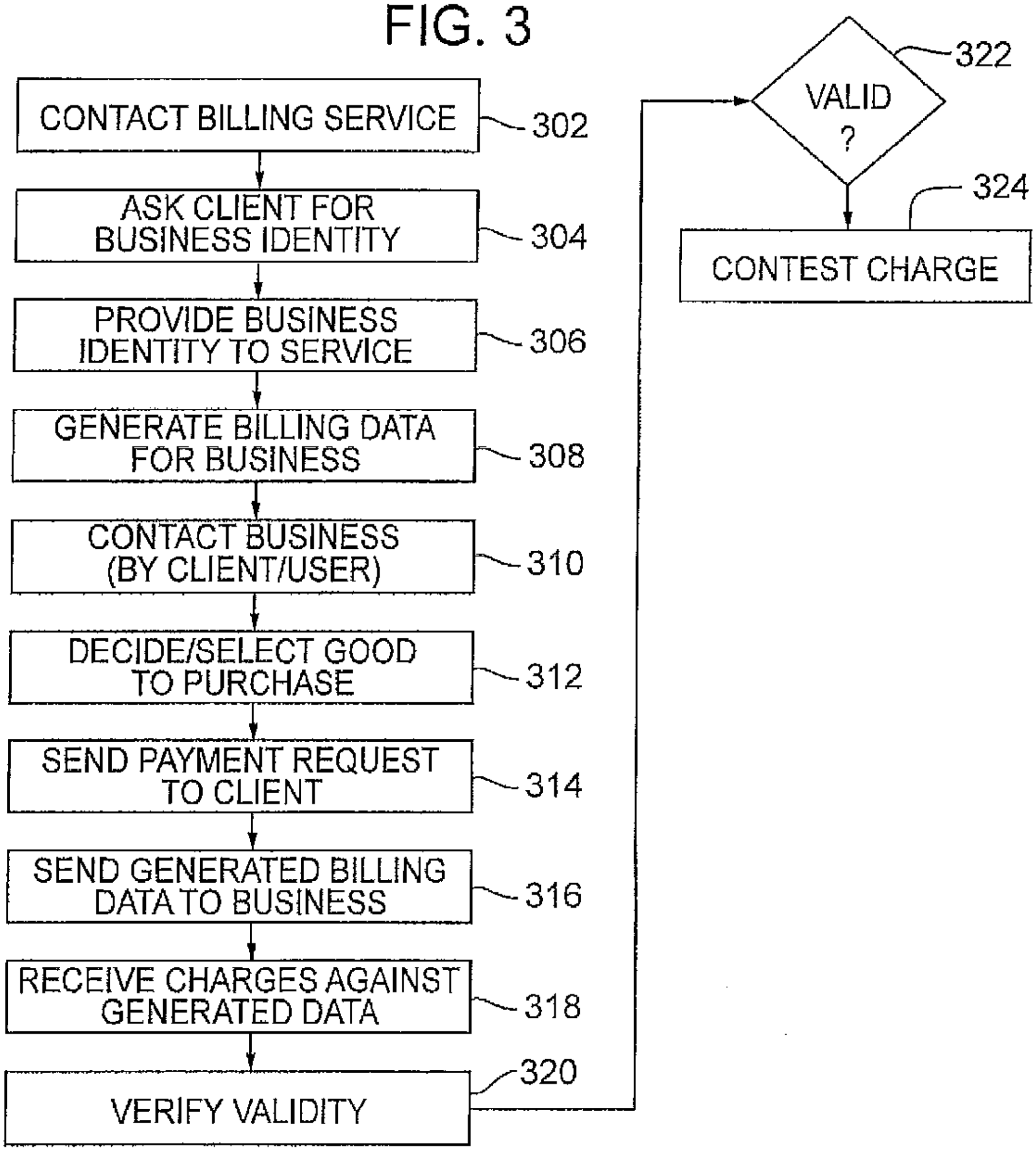
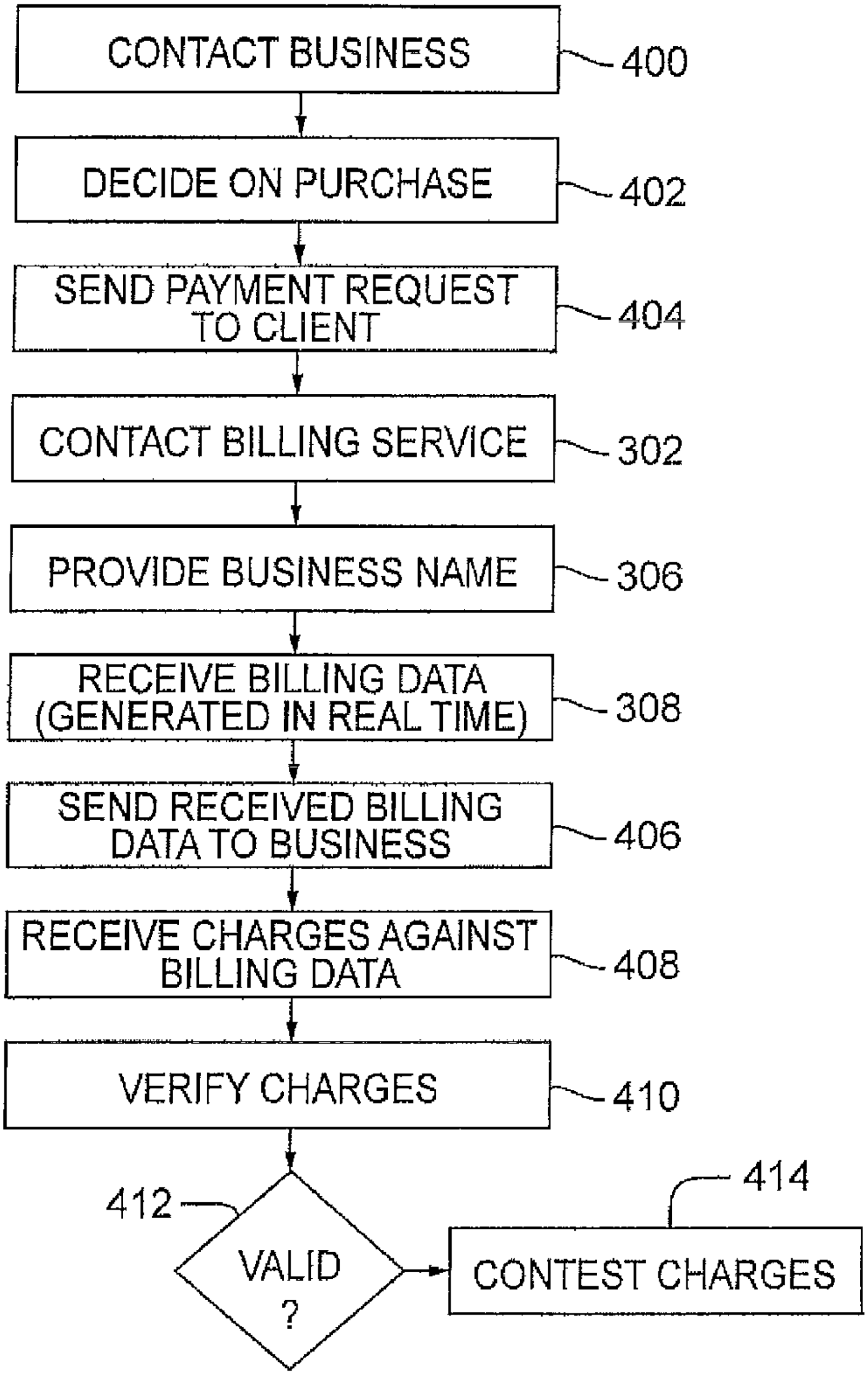

CONTACT BILLING SERVICE
302
ASK CLIENT FOR BUSINESS IDENTITY
304
PROVIDE BUSINESS IDENTITY TO SERVICE
306
GENERATE BILLING DATA FOR BUSINESS
308
CONTACT BUSINESS (BY CLIENT/USER)
310
DECIDE/SELECT GOOD TO PURCHASE
312
SEND PAYMENT REQUEST TO CLIENT
314
SEND GENERATED BILLING DATA TO BUSINESS
316
RECEIVE CHARGES AGAINST GENERATED DATA
318
VERIFY VALIDITY
320
VALID ?
322
CONTEST CHARGE
324

FIG. 4


CONTACT BUSINESS
400
DECIDE ON PURCHASE
402
SEND PAYMENT REQUEST TO CLIENT
404
CONTACT BILLING SERVICE
302
PROVIDE BUSINESS NAME
306
RECEIVE BILLING DATA (GENERATED IN REAL TIME)
308
SEND RECEIVED BILLING DATA TO BUSINESS
406
RECEIVE CHARGES AGAINST BILLING DATA
408
VERIFY CHARGES
410
412
VALID ?
414
CONTEST CHARGES

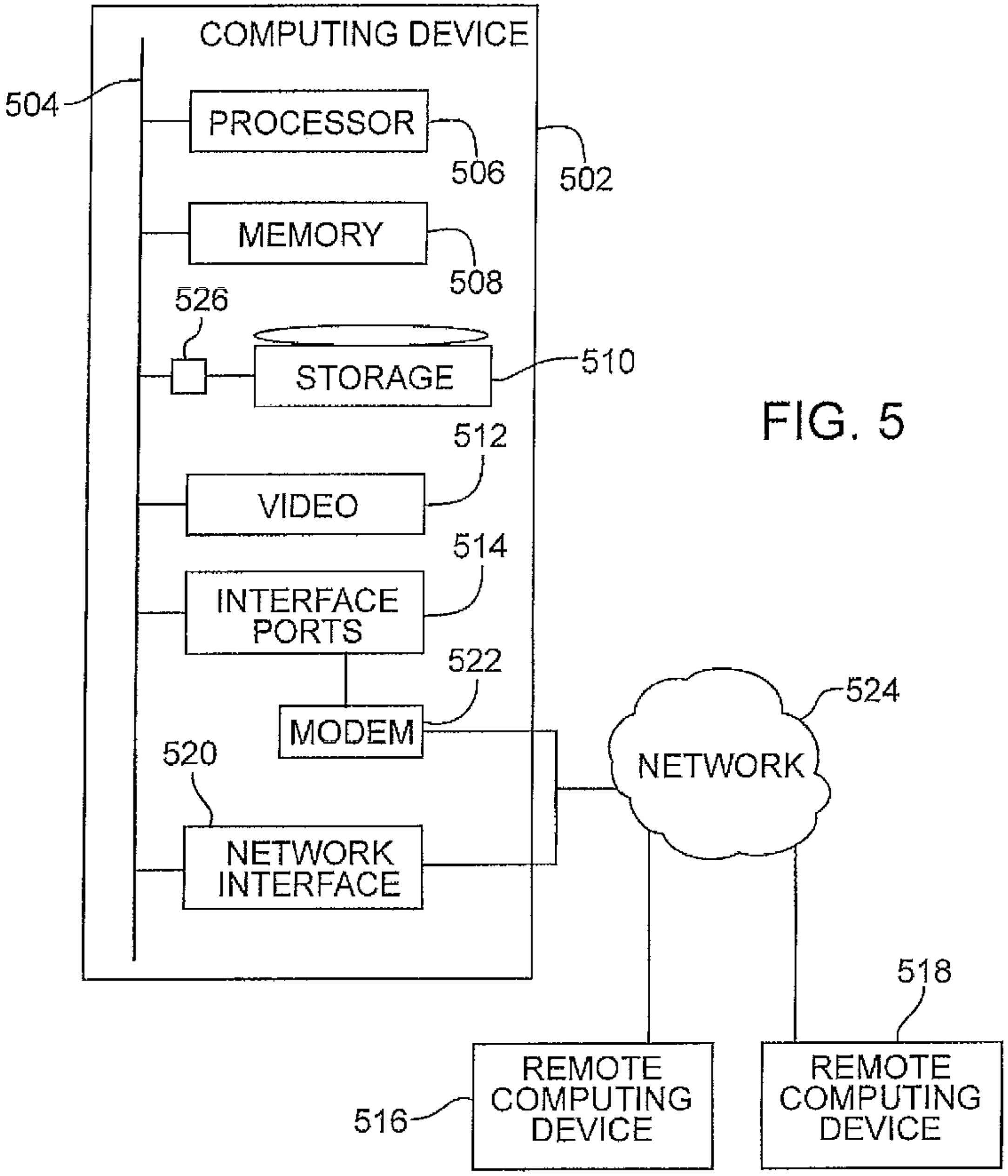

COMPUTING DEVICE
504
PROCESSOR
506
502
MEMORY
508
526
STORAGE
510
512
VIDEO
514
INTERFACE PORTS
522
524
MODEM
NETWORK
520
NETWORK INTERFACE
518
REMOTE COMPUTING DEVICE
516
REMOTE COMPUTING DEVICE

FIG. 5

MASKING PRIVATE BILLING DATA BY ASSIGNING OTHER BILLING DATA TO USE IN COMMERCE WITH BUSINESSES

CROSS-REFERENCE TO RELATED APPLICATIONS

The present patent application is a divisional of and claims priority from U.S. patent application Ser. No. 09/553,068, filed Apr. 20, 2000, the entire disclosure of which is hereby incorporated by reference as if fully set forth herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of information systems. More specifically, the present invention relates to electronic purchases while maintaining privacy of customer billing data.

2. Background Information

The Internet is a well-known collection of public and private data communication and multimedia networks that operate using common protocols to form a world wide network of networks. Recently there has been an explosion in the availability of "virtual storefronts," e.g., commerce sites, reachable over the Internet. This rapid growth is due, in part, to the availability of fast, reliable and affordable computing device systems, and the general simplification of networking hardware and configuration. Thus, consumers and businesses alike now have access to hardware that makes effective online commerce commercially practicable.

To conduct online transactions, a business typically sets up a home page (e.g., "web site") on the World Wide Web, which is a logical overlay of the Internet. Web sites are simply machines located someplace within the Internet, with traditional naming conventions for the machines, e.g., named WWW, and holding themselves available to interact using standard protocols such as Hypertext Transfer Protocol (HTTP), and programming languages or environments such as Hypertext Transfer Protocol HTML, XML, Java, JavaScript, Java Beans, ActiveX, Visual Basic, or the like.

To make a purchase via a web site, a customer executes a "browser," such as the Internet Explorer, Netscape Navigator, or other network aware application program that is configured to communicate with a business' web site. The customer locates a particular product, and proceeds to a "check out" web page (or equivalent) to process a purchase transaction. At this point, the customer must enter credit card data and other data sufficient to identify the customer and allow purchase of goods to occur.

Historically, thieves have attempted to monitor such online transactions so as to steal consumer data to allow engaging in subsequent fraudulent transactions. Such monitoring is possible due to the inherently insecure nature of the Internet communication protocol. Internet communication follows the Transmission Control Protocol/Internet Protocol (TCP/IP), where data is broken into small packets that are individually sent to a recipient, received by the recipient and then re-assembled into the original data.

Unfortunately, anyone with access to a network has the ability to "snoop" network traffic on that network. Thus, anyone capable of monitoring some portion of the communication path between the customer and business is then able to monitor the purchase transaction. To overcome this security problem, various protocols, e.g., IP Security (IPSEC), Secure Sockets Layer (SSL), Secure HTTP (S-HTTP) have emerged to allow a business and a customer to securely communicate.

Although the data packets can still be snooped, their contents are now encrypted and unusable. Thus, thieves have recently begun to attack, or "hack," the online commerce sites so as to steal consumer data stored within databases maintained by the business. Since private consumer data, such as credit card information, once received by a business, is reassembled and decrypted by the business, the data is available for theft.

Thus, what is needed is an environment which provides consumers with the ability to engage in online transactions in a more secure manner.

SUMMARY

Apparatuses and methods registering a user with multiple businesses, where each business is given billing data, such as credit card data, that is unique to that business. Apparatuses, such as computing devices, and consumer electronic devices such as a telephone, communicate with a billing service so that billing data can be generated for particular businesses and used in commercial transactions with the business. Such communication and generation may be in advance of a purchase, or generated in real-time during a purchase.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a client in communication with a network.

FIG. 2 is a flow chart according to one embodiment of the invention, illustrating a client registering with a business for purchasing a good.

FIG. 3 is a flowchart according to one embodiment of the invention, in which a client purchases a good using billing data provided in advance by a billing service.

FIG. 4 is a flowchart according to one embodiment of the invention, in which a client purchases a good using billing data provided in real-time by a billing service.

FIG. 5 illustrates one embodiment of a suitable computing environment in which certain aspects of the illustrated invention may be implemented.

DETAILED DESCRIPTION

In various embodiments of the invention, a customer is able to establish accounts with web sites without revealing private billing information such as credit card numbers, advance debit arrangements, invoice arrangements, etc. to a web site/business from whom the customer purchases goods.

FIG. 1 illustrates a client 100 in communication with a network 104. Also attached to the network are multiple servers 102 (business web sites), such as those provided by e-commerce sites, online retailers, or other businesses seeking to engage in commerce with by way of networked customers.

It is assumed the client comprises a computing device, such as a personal computer, which operates on behalf of a user (the purchaser of the good). In alternate embodiments, the client may be incorporated into an electronic card, a telephone (FIG. 6), a personal digital assistant (PDA), a portable audio device, a portable audiovisual device, a cellular telephone, a key-chain dongle, or within an automobile or other transportation device.

It is further assumed that each of the network locations to which a client may communicate provide a "web site" for engaging in commercial transactions, and will collectively be referred to as "businesses." For the purposes of this description, the phrase "web site" is intended to be a general reference to a network "presence" maintained by a business as well a logical presence maintained on behalf of a business.

The clients 100 and businesses 102 are in communication, through the network 104, with a billing service 106. The billing service is configured to allow clients 100 to reduce the risk of disclosing billing data, such as personal credit card numbers, debit card numbers, bank account numbers, and the like, to businesses 102. In one embodiment, the billing service facilitates commercial transactions by generating substitute billing data that the client 100 can use when engaging in commercial transactions with businesses 102. The phrase "substitute billing data" refers to valid billing data that is owned and/or controlled by the billing service 106, where billing data is temporarily or permanently distributed to clients 100 to replace personal and/or private billing data of the client.

Also in communication with the client 100 and businesses 102 by way of the network 104, is an encryption server 108. The encryption server can be used to provide encryption keys to a client 100 and business 102 to allow them to engage in secure communications. In one embodiment, the encryption server 108 is used to engage in conventional public key encryption systems, where the encryption server provides directory assistance services, allowing clients 100 and businesses 102 to retrieve public encryption keys.

In one embodiment, public key encryption services are used in addition to encryption services already available to a client (e.g., such as those available within a web browser or other communication program used by the client 100). In an alternate embodiment, already available encryption services, such as those provided by a web browser, are used to securely communicate with the encryption server 108 to obtain encryption keys for opening a secure communication channel between the client 100 and business 102.

This allows weaker security afforded by the client communication environment, e.g., a 40 bit or other short key system, to be used to communicate with the encryption server 108 to obtain more secure (e.g., longer) encryption keys. In this alternate embodiment, the built in security can also be used to transfer non-public key based cryptosystem keys, such as single use session keys, to the client 100 and business 102 for engaging in commerce.

Associated with clients 100 are local storage, such as a database 110, that can store billing data and encryption data for use during transactions with a business 102. In one embodiment, records 112 within the database 110 are keyed on a business 102 identity reference. A business identity can be tracked by way of business name, unique identifier for the business (e.g., a tax ID or other assigned/selected identifier), uniform resource locator (URL), TCP/IP "dot quad" network address (e.g., 10.1.2.3) used to access the business 102 over the network 104, or a combination of these and/or other references.

As illustrated, the client local storage containing the database 110 is integral to a client 100, such as within local mass storage device(s). However, it will be appreciated that the database may be contained within a separate computing device (not shown) associated with the client 100, or maintained by or in conjunction with the billing service 106 or encryption server 108. For example, the billing service 106 or encryption server 108 may be used to store backup copies of billing data.

FIG. 2 is a flow chart according to one embodiment of the invention, illustrating a client 100 registering with a business 102 for purchasing a good (e.g., a physical or electronic item) from the business.

The first illustrated operation is the user initializing 200 the computing device. It is assumed that initialization includes all steps required to boot, wake from an idle state, or otherwise start the computing device and configure it for purchasing activity. Assume that the computing device is a handheld ("palmtop") personal computer executing the Microsoft Windows operating system. After initialization, the user loads 202 a communication program through which to engage in the purchasing activity.

It will be appreciated that a number of environments may be used to implement the communication program. For example, a dedicated/custom application program may be designed to access businesses over a network. Alternatively, the communication program can be built using communication features provided by Internet web browser products, such as Microsoft Internet Explorer, Netscape Navigator, or Opera.

In this latter environment, the communication program may be implemented in one of, or a combination of, Java, JavaScript, JavaBeans, ActiveX, Visual Basic, HTML, DHTML, or other Internet related programming environments. It is assumed herein the communication program is based on an Internet browser, and that traditional Internet related communication protocols (e.g., TCP/IP, HTML, etc.) are used to communicate with businesses over the Internet. As discussed with respect to FIG. 1, each business provides a web address to which a client can connect to engage in purchase transactions.

After communication program initialization, the computing device is used to register 204 the user with a first web site maintained by a first business. Note, however, that even though the illustrated embodiment requires registration, it will be appreciated that in other embodiments, such registration need not occur first, or at all. To register, the computing device contacts 206 the first web site. In response the web site sends an acknowledgement 208. Since an Internet browser is assumed in use, the contact is by way of directing the browser to an appropriate receiving port monitored by a web server of the first business. It is assumed that port 80, the traditional Internet communication port, is used for communication. In the web browser context, acknowledgement can be determined by receiving a "home page" or start page from the first business' web server.

If 210 no acknowledgement is received, then a registration error has occurred and processing of this registration halts 212; in one embodiment, processing continues on (not shown) with registration attempts with other businesses. If acknowledgement is received, then the client 100 tells the business 102 it is interested in registering with the business 102.

In one embodiment, the registration process is automated, where the business web server is configured to receive a registration command from the client, and in response the business web server sends the client registration forms to complete. For example, in response to the registration command, an HTML form (or equivalent structure) containing fields for the user's name, address, telephone number, and billing data, such as credit or debit card numbers, invoicing preferences, etc., is sent 214 to the client. This form (or equivalent structure) is completed 216 and returned 218 to the business. In response, the business 102 processes the returned data and registers 220 the client with the billing data returned 218 to the business web server.

Completion of the form can be automated, through automated parsing of the form to identify various fields to fill out. In one embodiment, the extensible markup language (XML) is used to encode forms with semantic meaning to facilitate automatic interpreting and completing of a form. In an alternate embodiment, the user is allowed to review and complete a form with data known to the user, or the user can be provided with an opportunity to review and change a form completed by the computing device. In another embodiment, a special communication port, analogous to browser port 80, is used to send and receive registration data.

It will be appreciated that even though the above description assumes registration of a user with businesses, such registration is not required in order to obtain billing data to present to such businesses.

FIG. **3** is a flowchart according to one embodiment of the invention, in which a client **100** purchases a good using billing data provided in advance by a billing service **106**. This figure concerns the logical data flow for obtaining billing data used by a client **100** in purchasing a good from a business **102**.

As discussed above, there are intrinsic security issues within networks, such as the Internet or home/office local area networks (LANs), when more than just the parties to a conversation may "snoop" data passing on the network so as to discover secrets (e.g., credit card data or other sensitive data) disclosed during the conversation. In addition to attempts to securely encrypt the data transfers themselves, as will be discussed below, client provided billing data can be customized so as to reduce risk of theft and/or fraudulent use.

A first operation is to contact **302** the billing service. In response, the billing service asks **304** for the business **102** with which the customer seeks to interact. As discussed above, a variety of different information can be provided to identify the business. For simplicity, it is assumed that the business name is used to identify the business **102**. The business name is provided **306** to the billing service **106**. In response the billing service generates **308** billing data that can be used by the client in future transactions between the client and the identified business. The correspondence between billing data and business is tracked by the client **100** and/or it is tracked by the billing service **106**.

Once the billing data is known, the client **100** can then contact **310** a business and decide **312** on a good to purchase. In response to a purchase decision, the business sends **314** a payment request to the client to arrange for receiving payment for the good. However, unbeknownst to the business **102**, in response to the payment request, instead of sending personal credit card information, or other payment data, the client **100** instead sends **316** the business the billing data created in advance by the billing service for the business **102**.

In one embodiment, the billing service obtains the billing data to distribute to clients by entering into agreements with banking institutions (or equivalent). The billing service is provided a large number different billing data, e.g., credit card numbers, debit card numbers, etc., and the billing service may also set up internal invoice accounts and the like. These different billing data are provided to a client **100** when the client registers with the billing service the client's intent to purchase from a business **102**.

In one embodiment, billing data presented to a client **100** is uniquely associated with the particular business **102** the client **100** intends to purchase from. Charges made against the billing data are received **318** by the billing service in due course through standard financial institutions such as banks, savings and loans, investment houses, and the like. These charges are verified **320** for validity.

In one embodiment, the client informs the billing service of the items purchased (or possibly just item categories) so that the billing service may audit a particular charge to ensure only expected purchases appear on the charge. In one embodiment, the client informs the billing service of billing data that is provided to businesses so as to facilitate verification. For example, the origin of a charge can be compared against the business associated with the billing data.

In this embodiment, if **322** the charge origin fails to match the business expected to be making the charge, then the charge may be fraudulent. Consequently, the charge is contested **324** so as to allow the client to investigate the validity of the charge before being billed for the charge. However, if **322** the expected business matches the charge origin, then the client is billed for the purchase amount paid by the billing service. Note that the client may be billed in a manner entirely different from the payment system required/used by the business **102**.

For example, the client may have arranged to have purchases automatically deducted from a bank account, while the billing service **106** is responsible for honoring a charge made by the business against credit card data provided by the client **100**. Alternatively, the client may have arranged payment such that the billing service performs a direct wire transfer from a client's bank account directly into a receivables account of the business **102**.

By associating a particular business with billing data, it is possible to account for a thief stealing apparently valid billing data from a business' Internet web server, and then attempting to engage in fraudulent activity. In addition to contesting **324** improper charges, the billing service can be configured to retire billing data that has been compromised.

FIG. **4** is a flowchart according to one embodiment of the invention, in which a client **100** purchases a good using billing data provided in real-time by a billing service **106**. It will be appreciated that even though FIGS. **3** and **4** are presented separately, a single client may use both real-time generated billing data, and advance-obtained billing data, depending on the business.

After contacting **400** a business **102** from which a purchase is to be made, the client **100** user decides **402** on the purchase; this decision is transmitted to the business. It will be appreciated that this decision-making process may include the user reviewing various offerings of the business **102** (e.g., "surfing" the business web site), as well as directly connecting to a particular uniform resource location (URL) for purchasing a product (a purchase link may be known in advance).

In response to the purchase decision, the business **102** sends **404** a payment request to the client. In response, analogous to that described above for FIG. **3**, the client contacts **302** the billing service **106**, provides **306** the business name to the service, and receives in real time billing data generated **308** by the billing service for the business **102**. In one embodiment, the billing data presented to the client **100** is uniquely associated with the particular business **102** the client **100** is purchasing from.

As with FIG. **3**, unbeknownst to the business **102**, in response to the payment request **404**, instead of sending personal billing information of the user, the real time generated billing data is instead sent **406** to the business.

Charges made against the billing data are received **408** by the billing service. As with FIG. **3**, these charges are verified **410** for validity. If **412** the charges appear invalid/fraudulent, the charge may be automatically contested **324** or other action taken, such as highlighting the transaction to the user to allow review of the validity of the charge.

If **412** the charge is valid, then the client is billed for the purchase amount paid by the billing service. Note that the client may be billed in a manner entirely different from the payment system required/used by the business **102**. In one embodiment, highlighting occurs within the bill sent to the user to accentuate invalid or possibly invalid charges. Highlighting can be by a variety of different methods, such as printing an offending charge in a bold typeface, in a larger type size, in a different font from the rest of the bill, in a different color, in a different section of a bill which organizes suspect charges in a single region, or through a combination of these or other highlighting techniques.

In one embodiment, the billing service 106 tracks expiration dates for charges made by the user. That is, if a charge is received against a credit card number provided to a client 100 for purchasing from a business 102, there may be a timeout period, such as 60 days, in which a charge must be contested if such charge is to be ever contested. In such circumstances, the highlighting may include prioritization of listed charges according to expiration of contest periods. In another embodiment, a separate bill section is provided for contestable charges expiring within a certain amount of time, such as two weeks.

In one embodiment, the client can elect to be billed electronically, in addition to or in lieu of receiving a physical bill printed on paper. Electronic billing can be by way of E-mailing or otherwise electronically transferring bill data to the client. Alternatively, bills can be maintained by the billing service 106, such as through personalized web pages to which a client can log in and review charges. In one embodiment, the personalize web pages include buttons or other controls to allow disputing charges. In one embodiment, single-click buttons are provided with listed charges, where a single click of the button institutes a dispute process to cause the selected charge to be reviewed for fraud.

FIG. 5 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which certain aspects of the illustrated invention may be implemented. The invention may be described by reference to different high-level program modules and/or low-level hardware contexts. Those skilled in the art will realize that program module references can be interchanged with low-level hardware instructions.

Program modules include procedures, functions, programs, components, data structures, and the like, that perform particular tasks or implement particular abstract data types. The modules may be incorporated into single and multiprocessor computing systems, as well as hand-held devices and controllable consumer devices (e.g., Personal Digital Assistants (PDAs), cellular telephones, set-top boxes, Internet appliances, etc.). It is understood that modules may be implemented on a single computing device, or processed over a distributed network environment, where modules can be located in both local and remote memory storage devices.

An exemplary system for implementing the invention includes a computing device 502 having system bus 504 for coupling together various components within the computing device. The system 504 bus may be any of several types of bus structures, such as PCI, AGP, VESA, Microchannel, ISA and EISA, etc. Typically, attached to the bus 504 are processors 506 such as Intel, DEC Alpha, PowerPC, programmable gate arrays, etc., a memory 508 (e.g., RAM, ROM), storage devices 510, a video interface 512, and input/output interface ports 514.

The storage systems and associated computer-readable media provide storage of data and executable instructions for the computing device 502. Storage options include hard-drives, floppy-disks, optical storage, magnetic cassettes, tapes, flash memory cards, memory sticks, digital video disks, and the like, and may be connected to the bus 504 by way of an interface 526.

Computing device 502 is expected to operate in a networked environment using logical connections to one or more remote computing devices 516, 518 through a network interface 520, modem 522, or other communication pathway. Computing devices may be interconnected by way of a network 524 such as a local intranet or the Internet. Thus, for example, with respect to the illustrated embodiments, assuming computing device 502 is a client seeking to purchase goods, then remote devices 516, 518 may be a billing service 516 providing substitute billing data to the user for purchasing goods from a business 518.

It will be appreciated that remote computing devices 516, 518 may be configured like computing device 502, and therefore include many or all of the elements discussed for computing device 502. It should also be appreciated that computing devices 502, 516, 518 may be embodied within a single device, or separate communicatively-coupled components, and include routers, bridges, peer devices, web servers, and application programs utilizing network application protocols such as HTTP, File Transfer Protocol (FTP), Gopher, Wide Area Information Server (WAIS), and the like.

Having described and illustrated the principles of the invention with reference to illustrated embodiments, it will be recognized that the illustrated embodiments can be modified in arrangement and detail without departing from such principles.

And, even though the foregoing discussion has focused on particular embodiments, it is understood that other configurations are contemplated. In particular, even though expressions such as "in one embodiment," "in another embodiment," and the like are used herein, these phrases are meant to generally reference embodiment possibilities, and are not intended to limit the invention to particular embodiment configurations.

As used herein, these terms may reference the same or different embodiments, and unless expressly indicated otherwise, are combinable into other embodiments. Consequently, in view of the wide variety of permutations to the above-described embodiments, the detailed description is intended to be illustrative only, and should not be taken as limiting the scope of the invention. What is claimed as the invention, therefore, is all such modifications as may come within the scope and spirit of the following claims and equivalents thereto.

What is claimed is:

1. A method for a user to provide substitute billing data in lieu of personal billing data, comprising:

an electronic device facilitating a request to a billing service for first and second distinct credit card numbers, including identifying each business with which the first and second distinct credit card numbers are to be used;

the electronic device obtaining the first and second distinct credit card numbers from the billing service for use by the user as a substitute for said personal billing data, the first and second distinct credit card numbers associated with each said business by the billing service;

the electronic device facilitating one or more purchasing transactions with a first associated business using the first credit card number; and

the electronic device facilitating one or more purchasing transactions with a second associated business using the second credit card number.

2. The method of claim 1, wherein the electronic device is a portable digital assistant, said method further comprising:

the electronic device disposing said distinct credit card numbers in a memory within the electronic device;

the electronic device identifying a connection to, or a submitted request to connect to, a particular business;

the electronic device determining whether a selected credit card number associated with the particular business is present in the memory; and

if found in the memory, the electronic device displaying the selected credit card number for the particular business.

3. The method of claim 2, further comprising:

if no selected credit card number for the particular business is found, the electronic device then selecting a third credit card number from said distinct credit card numbers to facilitate purchasing transactions with the particular business; and

the electronic device automatically conveying to the billing service of said selection of said third credit card number to conduct purchasing transactions with the particular business.

4. The method of claim 1, wherein the method further comprises:

the electronic device notifying the billing service of said selection of said first and second distinct credit card numbers to facilitate purchasing transactions with said first and second businesses respectively, including identifying the first and second businesses for which the first and second distinct credit card numbers were selected.

5. A method comprising:

a billing service registering a user;

the billing service receiving identification of a first and a second business with which the user intends to conduct one or more purchasing transactions;

the billing service associating a first and a second billing data, that are separate and distinct, with the first and the second business respectively; and

the billing service providing the first and second billing data for use by the user as substitutes for personal billing data for subsequent purchasing transactions.

6. The method of claim 5, wherein said first billing data further comprises:

a third billing data for use by said first business for charging the billing service for goods purchased by said user; and

a fourth billing data for use by the billing service for billing the user for charges received from said first business.

7. The method of claim 5, further comprising:

the billing service providing in real time said first and second billing data to an electronic device used by the user,

wherein the electronic device is operable to purchase goods from said first and second businesses.

8. The method of claim 5, further comprising:

the billing service receiving notification of usage of said first and second billing data with said first and second businesses from an electronic device used by the user.

9. The method of claim 8, wherein said receiving notification comprises receiving a charge against one of said first and second billing data by a corresponding one of said first and second businesses.

10. An apparatus comprising:

a storage medium having stored therein a plurality of programming instructions designed to enable the apparatus, when the programming instructions are executed, to register a user, receive identification of a first and a second business with which the user intends to conduct one or more purchasing transactions, associate a first and a second billing data, that are separate and distinct, with the first and the second business respectively, and provide the first and second billing data for use by the user as substitutes for personal billing data when conducting purchasing transactions with the first and the second businesses; and

a processor coupled to the storage medium to execute the plurality of programming instructions.

11. The apparatus of claim 10, wherein said first billing data further comprises:

a third billing data used by said first business for charging the billing service for goods purchased by said user; and

a fourth billing data for use by the billing service for billing the user for charges received from said first business.

12. The apparatus of claim 10, wherein the programming instructions, when executed by said processor, enable the apparatus to:

provide in real time said first billing data to an electronic device operable to purchase goods from said first business.

13. The apparatus of claim 10, wherein the programming instructions, when executed by said processor, enable the apparatus to:

receive notification of usage of said first billing data with said first business from an electronic device used by a purchaser.

14. The apparatus of claim 13, wherein said receiving notification comprises receiving a charge against said first billing data, the charge being made by said first business.

15. An apparatus for a user to provide substitute billing data in lieu of personal billing data, comprising:

means for facilitating a request to a billing service for first and second distinct credit card numbers;

means for identifying each business with which the first and second distinct credit card numbers are to be used;

means for obtaining from the billing service the first and second distinct credit card numbers associated with each business for use by the user as a substitute for said personal billing data;

means for facilitating one or more purchasing transactions with a first associated business using the first credit card number; and

means for facilitating one or more purchasing transactions with a second associated business using the second credit card number.

16. The apparatus of claim 15, further comprising means for notifying the billing service of said selection of said first and second distinct credit card numbers to facilitate purchasing transactions with said first and second businesses respectively, and means for identifying the first and second businesses for which the first and second distinct credit card numbers were selected.

17. An article of manufacture including a computer-readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform a method comprising:

registering a user;

receiving identification of a first and a second business with which the user intends to conduct one or more purchasing transactions;

associating a first and a second billing data, that are separate and distinct, with the first and the second business respectively; and

providing the first and second billing data for use by the user as substitutes for personal billing data when conducting purchasing transactions with the first and the second businesses.

18. The article of manufacture of claim 17, wherein the instructions, if executed by the computing device, further cause the computing device to receive notification of usage of said first billing data with said first business from an electronic device used by a purchaser.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 7,664,701 B2	Page 1 of 1
APPLICATION NO.	: 11/591696	
DATED	: February 16, 2010	
INVENTOR(S)	: Phillips et al.	

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page:

The first or sole Notice should read --

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 344 days.

Signed and Sealed this

Thirtieth Day of November, 2010

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office

US007603382B2

(12) **United States Patent**
Halt, Jr.

(10) **Patent No.:** **US 7,603,382 B2**
(45) **Date of Patent:** **Oct. 13, 2009**

(54) **ADVANCED INTERNET INTERFACE PROVIDING USER DISPLAY ACCESS OF CUSTOMIZED WEBPAGES**

(76) Inventor: **Gerald B. Halt, Jr.**, 2252 E. Deerfield Dr., Media, PA (US) 19063

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 550 days.

(21) Appl. No.: **10/982,574**

(22) Filed: **Nov. 5, 2004**

(65) **Prior Publication Data**

US 2005/0097095 A1 May 5, 2005

Related U.S. Application Data

(63) Continuation of application No. 09/318,917, filed on May 26, 1999, now Pat. No. 6,816,849.

(60) Provisional application No. 60/086,671, filed on May 26, 1998.

(51) **Int. Cl.**
G06F 17/30 (2006.01)

(52) **U.S. Cl.** 707/104.1; 715/205; 715/234

(58) **Field of Classification Search** 707/104.1, 707/102, 101, 200; 715/200, 205, 234, 760
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,813,006	A		9/1998	Polnerow et al.	
5,819,271	A		10/1998	Mahoney et al.	
5,898,836	A	*	4/1999	Freivald et al.	709/218
5,960,411	A		9/1999	Hartman et al.	
5,978,568	A		11/1999	Abraham et al.	
6,009,410	A		12/1999	LeMole et al.	
6,029,141	A		2/2000	Bezos et al.	
6,035,119	A	*	3/2000	Massena et al.	717/100
6,041,360	A	*	3/2000	Himmel et al.	709/245
6,085,219	A	*	7/2000	Moriya	709/200
6,128,663	A	*	10/2000	Thomas	709/228
6,161,124	A		12/2000	Takagawa et al.	
6,175,831	B1		1/2001	Weinreich et al.	
6,178,424	B1		1/2001	Okumura et al.	
6,185,614	B1		2/2001	Cuomo et al.	
6,195,679	B1	*	2/2001	Bauersfeld et al.	709/203
6,208,986	B1		3/2001	Schneck et al.	
6,269,369	B1		7/2001	Robertson	
6,311,196	B1	*	10/2001	Arora et al.	715/209
6,369,819	B1	*	4/2002	Pitkow et al.	345/440
6,411,996	B1	*	6/2002	Albers	709/223
6,816,849	B1	*	11/2004	Halt, Jr.	707/1

OTHER PUBLICATIONS

Kristol et al., "HTTP State Management Mechanism", The Internet Engineering Taskforce, Feb. 1997, http://www.ietf.org/rfc/rfc2109.txt.

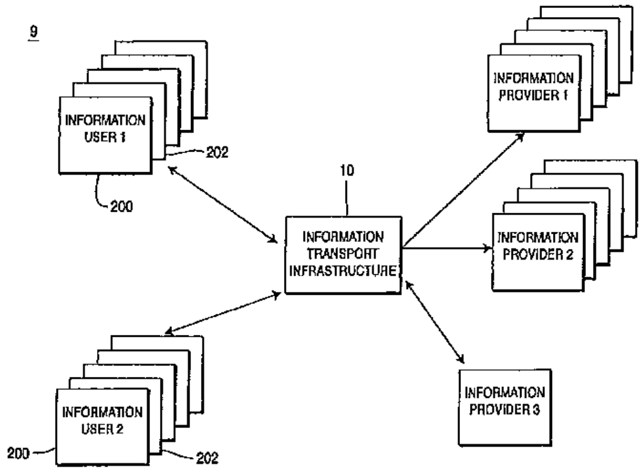
* cited by examiner

Primary Examiner—Cheryl Lewis
(74) *Attorney, Agent, or Firm*—Sterne Kessler Goldstein & Fox PLLC

(57) **ABSTRACT**

An Internet interface provided by an internet web server provides web pages presents in a manner which is tailored to an individual user. The interface provides web site navigation data to the user in accordance with personal preferences provided by the user. A site map program function then provides web site navigation data to the user, in order to provide a display depicting portions of the web site visited by the user.

23 Claims, 8 Drawing Sheets



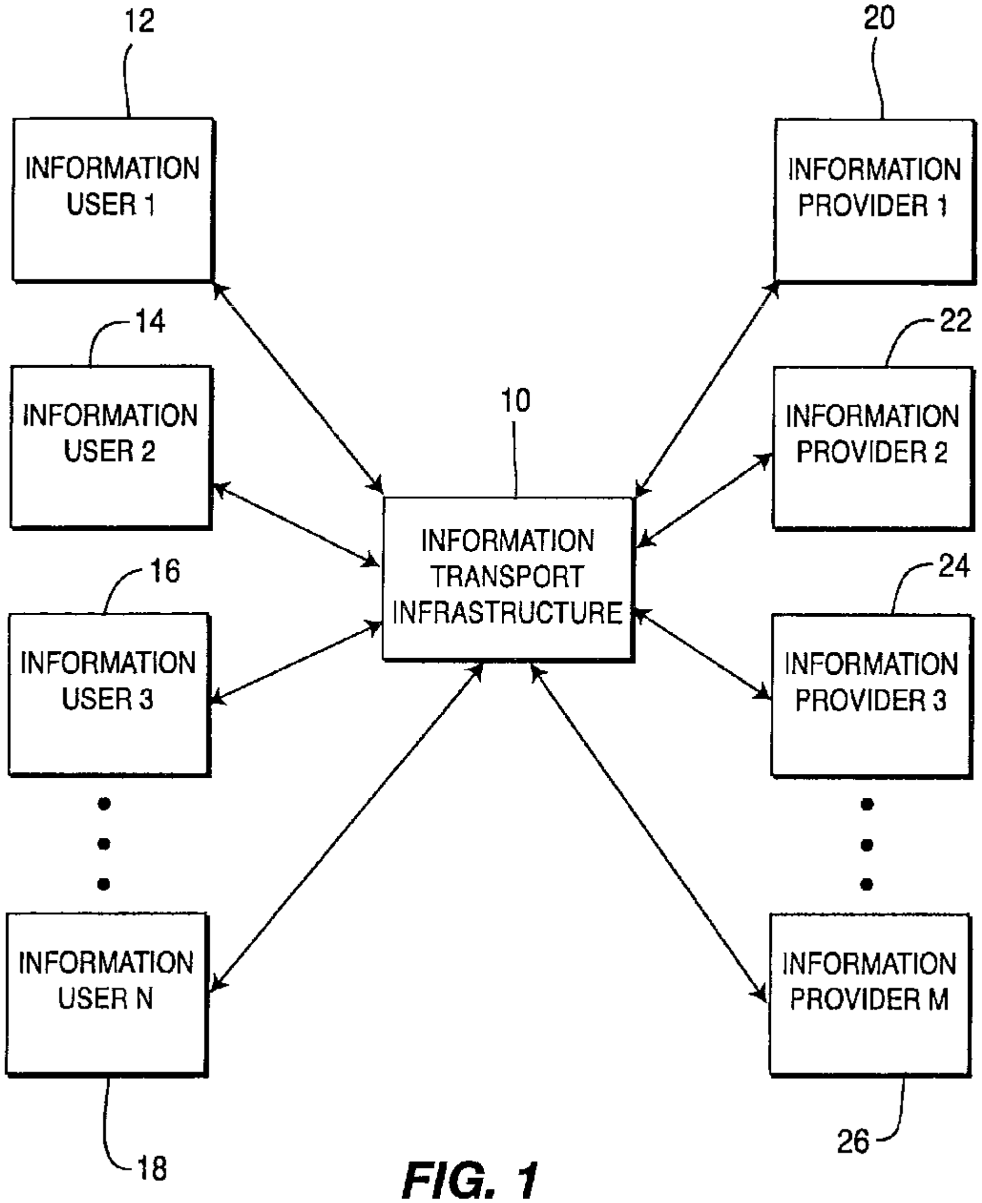


FIG. 1
PRIOR ART

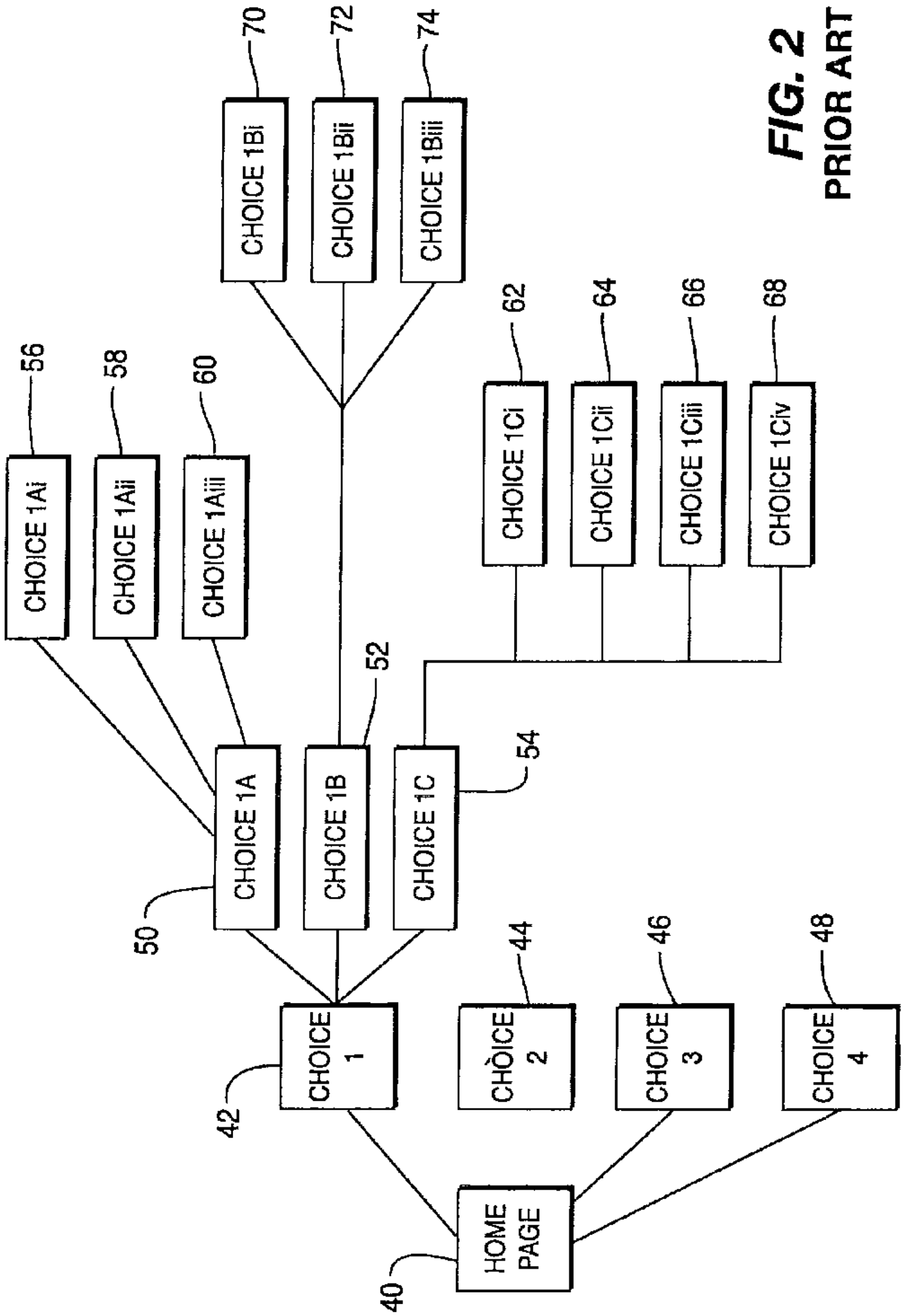


FIG. 2
PRIOR ART

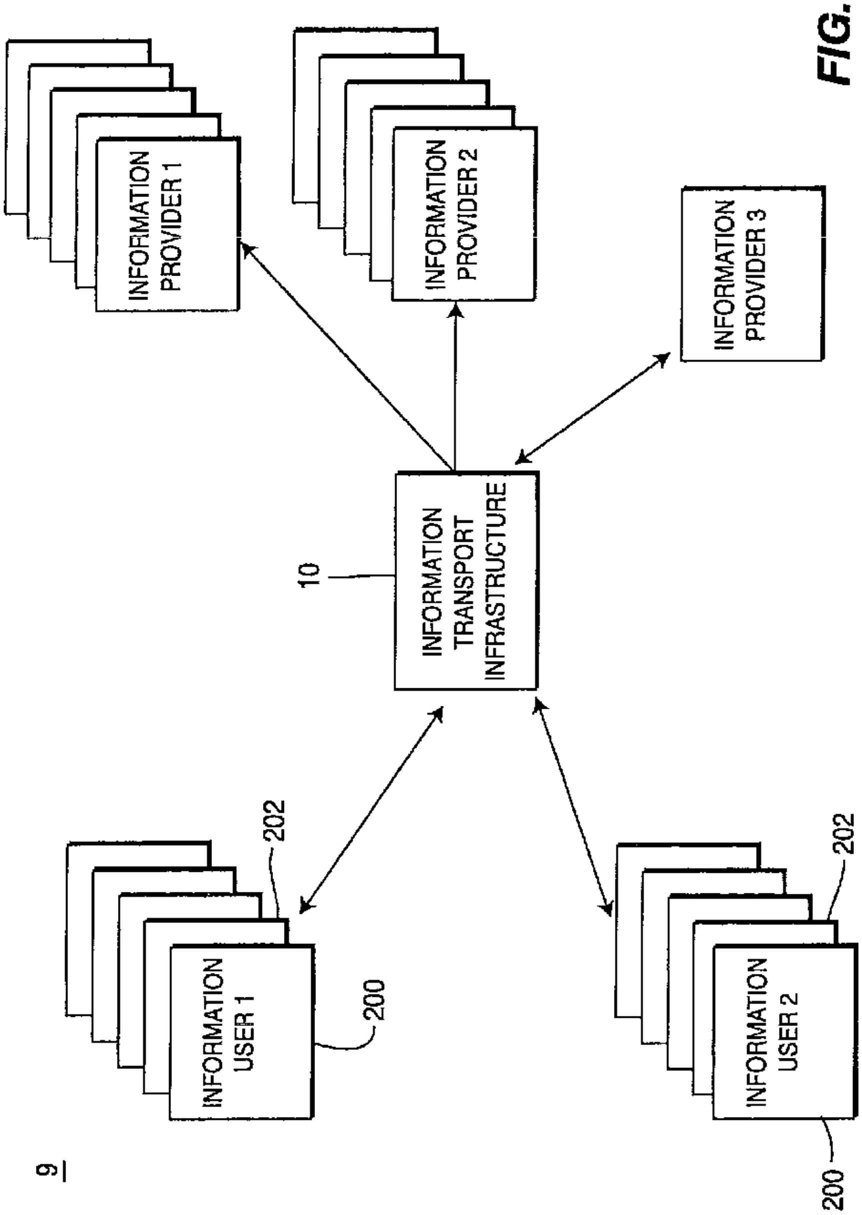

6
INFORMATION PROVIDER 1
INFORMATION PROVIDER 2
INFORMATION PROVIDER 3
10
INFORMATION TRANSPORT INFRASTRUCTURE
INFORMATION USER 1
202
200
INFORMATION USER 2
202
200

FIG. 3

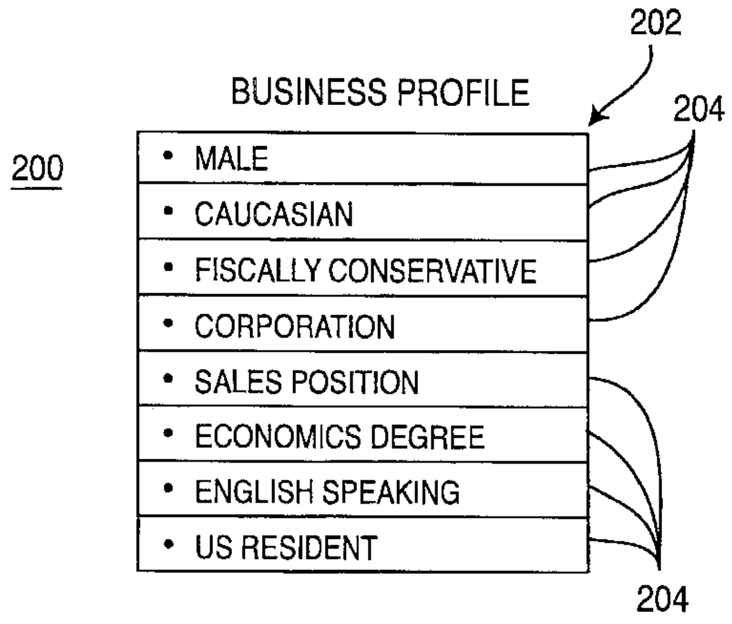

200
202
BUSINESS PROFILE
204
• MALE
• CAUCASIAN
• FISCALLY CONSERVATIVE
• CORPORATION
• SALES POSITION
• ECONOMICS DEGREE
• ENGLISH SPEAKING
• US RESIDENT
204

FIG. 4A

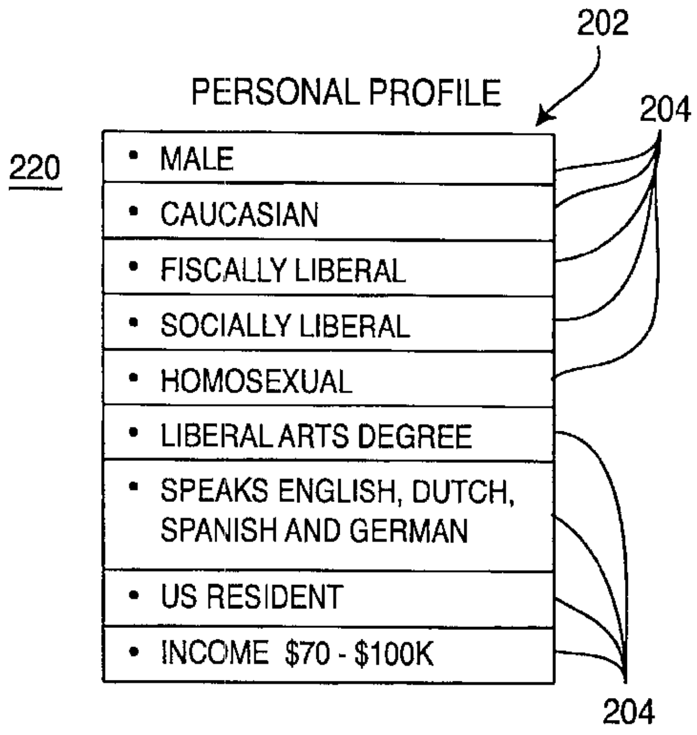
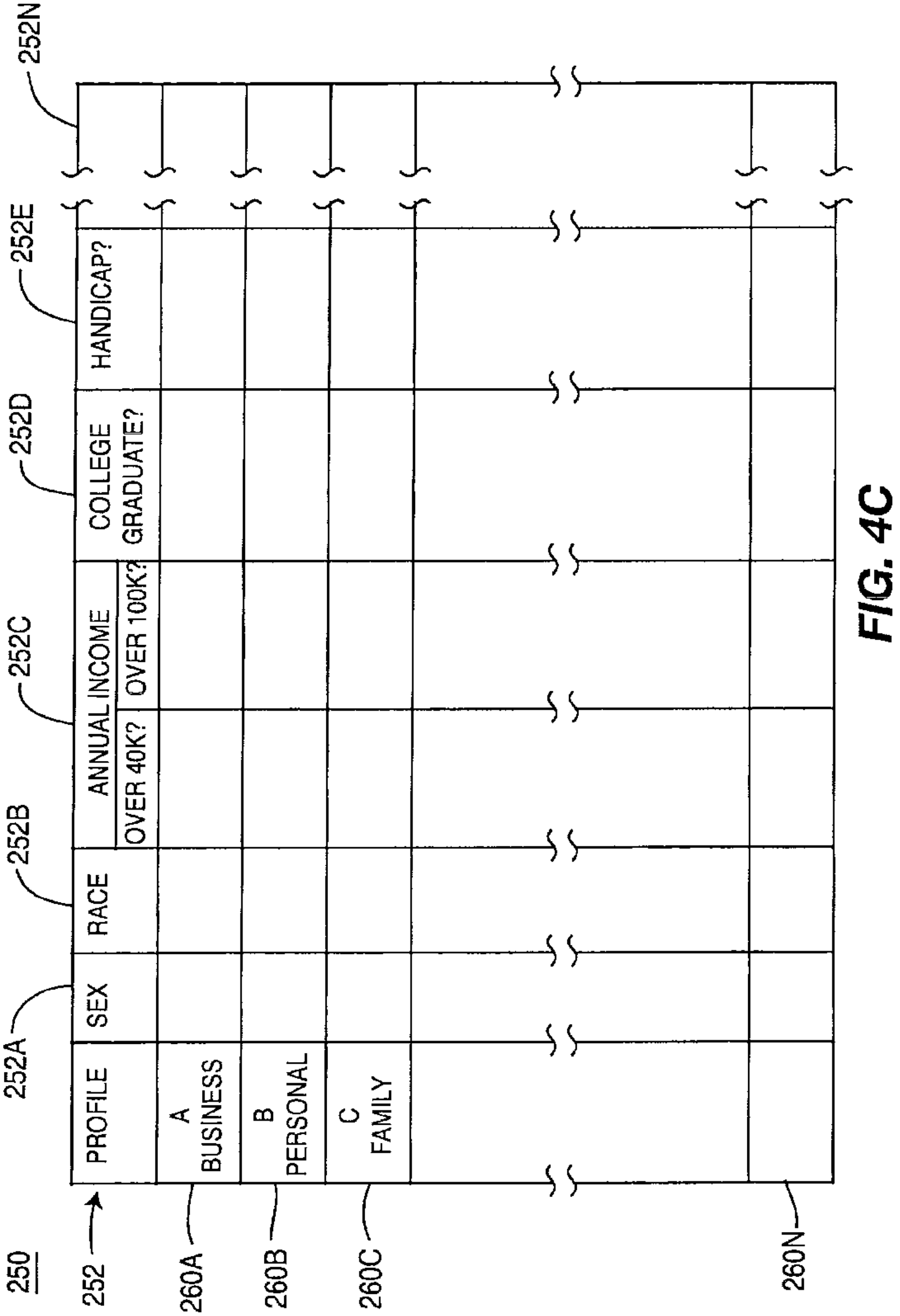

220
202
PERSONAL PROFILE
204
• MALE
• CAUCASIAN
• FISCALLY LIBERAL
• SOCIALLY LIBERAL
• HOMOSEXUAL
• LIBERAL ARTS DEGREE
• SPEAKS ENGLISH, DUTCH, SPANISH AND GERMAN
• US RESIDENT
• INCOME $70 - $100K
204

FIG. 4B



PROFILE	SEX	RACE	ANNUAL INCOME		COLLEGE GRADUATE?	HANDICAP?	
			OVER 40K?	OVER 100K?			
A BUSINESS							
B PERSONAL							
C FAMILY							

FIG. 4C

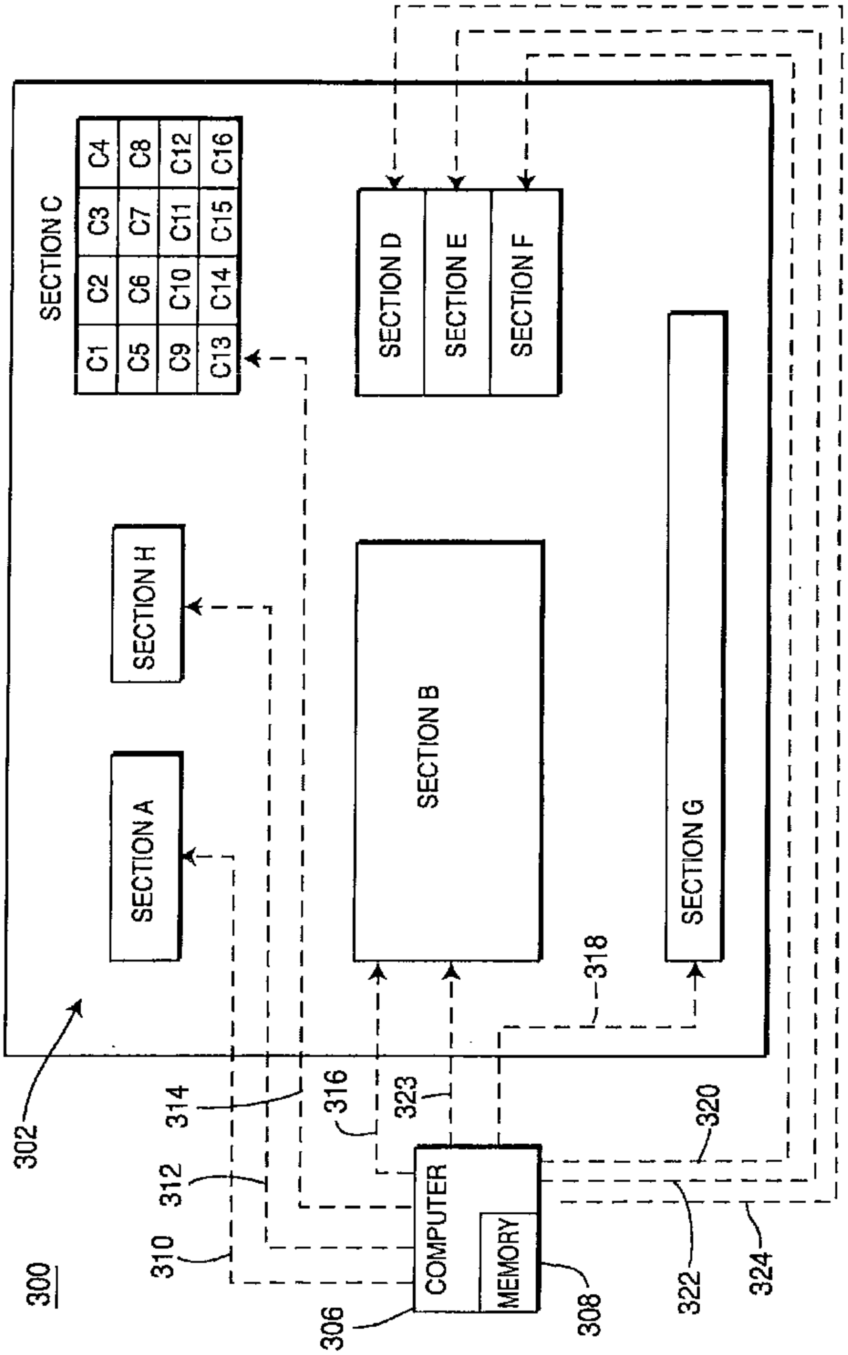
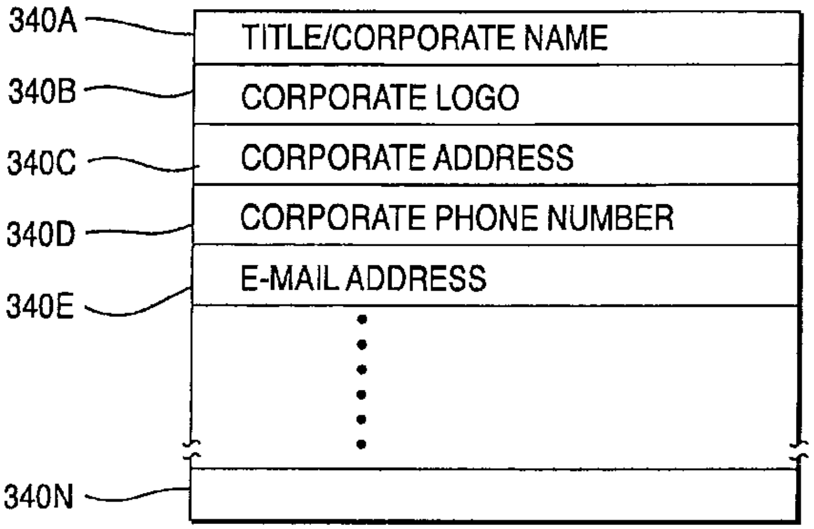

300
302
SECTION A
SECTION H
SECTION C
C1
C2
C3
C4
C5
C6
C7
C8
C9
C10
C11
C12
C13
C14
C15
C16
SECTION D
SECTION E
SECTION F
SECTION B
SECTION G
318
314
316
323
320
312
310
COMPUTER
MEMORY
306
308
322
324

FIG. 5A



TITLE/CORPORATE NAME

CORPORATE LOGO

CORPORATE ADDRESS

CORPORATE PHONE NUMBER

E-MAIL ADDRESS

FIG. 5B

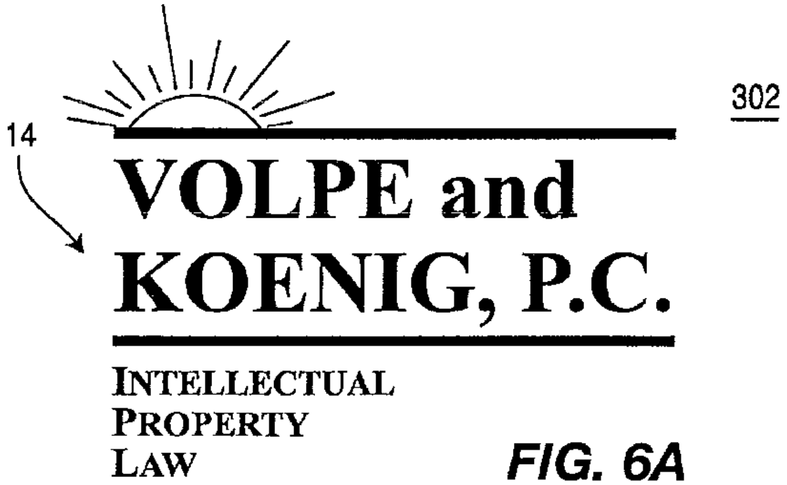


FIG. 6A

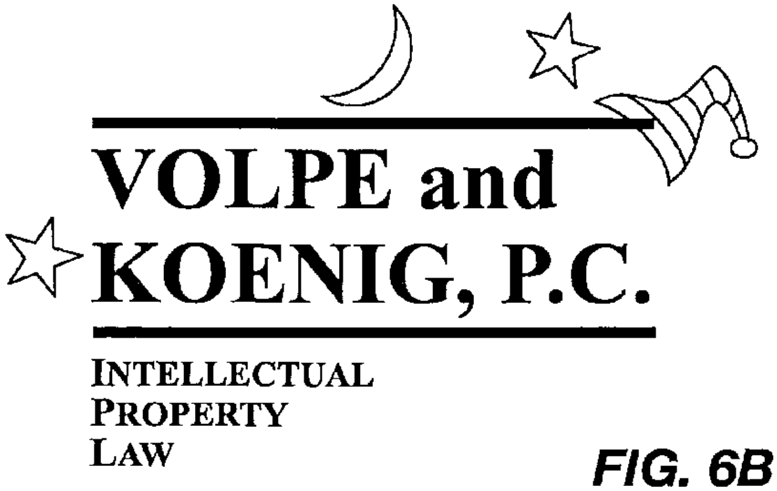


FIG. 6B

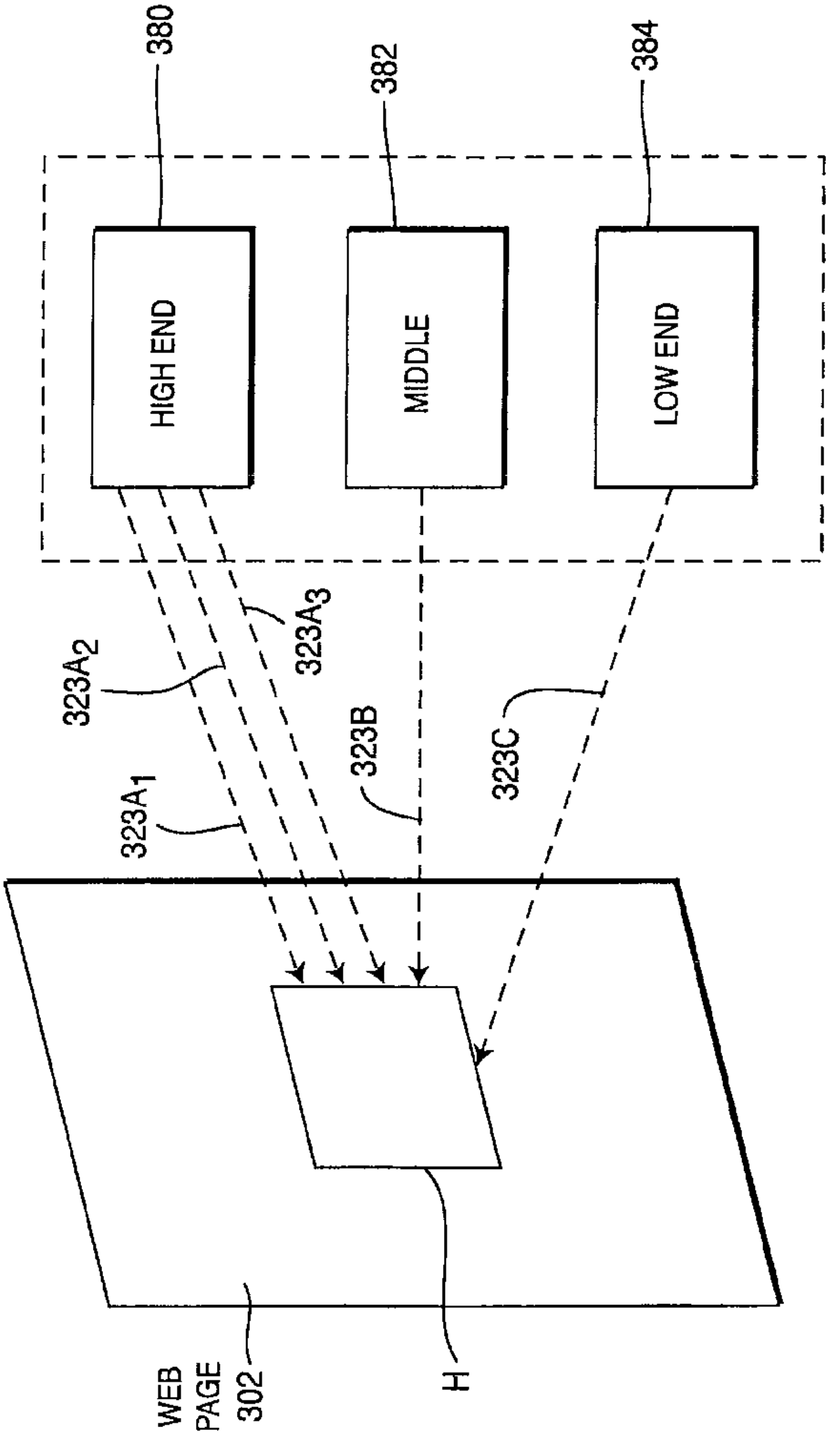

380
382
384
HIGH END
MIDDLE
LOW END
$323A_2$
$323A_3$
$323A_1$
323B
323C
WEB PAGE 302
H

FIG. 7

ADVANCED INTERNET INTERFACE PROVIDING USER DISPLAY ACCESS OF CUSTOMIZED WEBPAGES

CROSS REFERENCE TO RELATED APPLICATION(S)

This application is a continuation of U.S. patent application Ser. No. 09/318,917, U.S. Pat. No. 6,816,849, filed May 26, 1999, which in turn claims priority from U.S. provisional application No. 60/086,671 filed May 26, 1998, which are incorporated by reference as if fully set forth.

FIELD OF INVENTION

This invention pertains to the global computing network otherwise known as the Internet or the World Wide Web. More particularly, the invention pertains to a system for selectively tailoring information delivered to an Internet user depending upon the particular needs of the user.

BACKGROUND

The Internet is a global computer network that is rapidly changing the landscape of the business community and has begun change the way people perceive themselves as citizens of the global community. By its very nature, the Internet provides a flexible vehicle to deliver information from any point on the globe to any other point on the globe. Providing such a vast amount of information on demand is a feat which is unparalleled in history in both size and scope. However, due to the limitations inherent with computer hardware, modems and telephonic systems, only a small portion of the capabilities of the Internet are utilized today. As the performance of computer hardware and software catches up with the expectations of the Internet-using community, the applications for which the Internet is used will increase tremendously.

Use of the Internet is in its infancy. Much to the chagrin of the Internet-using community, the press constantly features articles and commentary on the Internet which is overly simplistic and misleading. Much of the capabilities of the Internet remain more hype than fact. Since evolution of the Internet is in its rudimentary stages, no one can predict where the frontier will lead.

One of the current problems with the Internet is that inexperienced people in the business community and the user community tend to view the Internet as a natural extension (or slight modification) of the currently existing media. For example, much of the public uses the Internet as a high tech phone book whereby a user can obtain detailed information regarding a company's products, services or other background information regarding a company. A perusal of home pages currently existing on the World Wide Web confirms that home pages are currently a hybrid of the business-to-business Yellow Pages® directory and a television commercial. The home pages are unable to obtain any information regarding the specific Internet users which are contacting the home page nor are they able to deliver information tailored specifically to that user without the user experiencing a tedious "virtual gauntlet" of boring questions that they must answer time and time again for each home page that is accessed. The initial enthusiasm and mystique associated with the Internet will quickly evaporate unless Internet users and the business community begin to utilize the Internet to its fullest potential.

Accordingly, there exists a serious need for delivering useful information to an Internet user that can be depended upon to deliver quality data as reliably as current utilities are delivered

SUMMARY

The present invention is a system for delivering information from an information provider to an information user that is selectively tailored toward the capabilities of the information provider and the needs of the information user. The system includes an interactive interface which provides a medium for information users to communicate with information providers. More specifically, the system includes means for the information user to tailor the profile of the information user depending upon the needs or desires of the information user. Separate means permit the information provider to view the information user profile and to structure the information seen by the information user in a format that is most suitable to that information user.

The system also enables the information user to operatively tailor their profile on a real time basis. Thus, the information provider may tailor the information provided to the Internet using community depending upon the time of day, business conditions or other factors.

Accordingly, it is an object of the present invention to provide an advanced Internet interface between Internet information users and Internet information providers.

Other objects and advantages will become apparent to those skilled in the art after reading the detailed description of a presently preferred embodiment.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of the interface between information users and information providers over the Internet according to the prior art.

FIG. **2** is a block diagram of the web page structures according to the prior art.

FIG. **3** is a block diagram of the interface between information users and information providers over the Internet according to the present invention.

FIGS. **4A-4C** are database structures of user information.

FIG. **5A** is a block diagram of information provider according to the present invention.

FIG. **5B** is a file structure of information identifiers according to the present invention.

FIGS. **6A** and **6B** are illustrations of web pages according to the present invention.

FIG. **7** is an illustration of a web page structure according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

The preferred embodiment will be described with reference to the drawing figures wherein like numerals represent like elements throughout.

A block diagram of the interface between current information users and information providers over the Internet is shown in FIG. 1. The information transport infrastructure **10** includes all of the infrastructure **10** required to convey information between the plurality of information providers **20, 22, 24, 26** and plurality of information users **12, 14, 16, 18**. This transport infrastructure **10** includes, but is not limited to, a wireless or wired public or private telephone system, a local area network (LAN) or a wide area network (WAN) upon which the information users **12, 14, 16, 18** or information providers **20, 22, 24, 26** are resident, the plurality of way stations in between, and all of the computing resources required to deliver the information. It should be recognized that this infrastructure **10** could include the local cable television (CATV) infrastructure, telephone company infrastructure or even the wires provided by the electric company over which information may be transmitted. It should also be recognized that the information may be transmitted by satellite or microwave means and the present example should not be viewed as a specific limitation upon the scope of the present invention.

As shown in FIG. 1, as each information user **12, 14, 16, 18** utilizes the Internet to access one or more information providers **20, 22, 24, 26**, each information provider **20, 22, 24, 26**, such as a Web page, will appear identical to each information user **12, 14, 16, 18**. There is no tailoring of information to each information user **12, 14, 16, 18**. Of course, an information user **12, 14, 16, 18** can run the aforementioned "virtual gauntlet" of questions to obtain the information they require, but this process is extremely frustrating and time consuming. Additionally, much of the information requested from the information user **12, 14, 16, 18** by an information provider **20, 22, 24, 26** is standard information such as an information user's name, address and other personal or financial information.

Most Web pages are structured as a logical tree and branch format as shown in FIG. 2. First, the information user **12, 14, 16, 18** accesses the desired home page **40**. As the information user **12, 14, 16, 18** inputs information and makes selections, the information user **12, 14, 16, 18** gains access to additional tiers of information. For example, if the first choice **42** is selected by information user **12, 14, 16, 18** on the home page **40**, the information user **12, 14, 16, 18** will be shown a second tier of choices **50, 52, 54**. Selection of the first choice **50** from this second tier of choices **50, 52, 54** will provide access to a third tier of information with three additional choices **56, 58, 60**. In this manner, the Web page **40** will provide incremental additional information in response to the selections made by the information user **12, 14, 16, 18**. Ultimately, the information user **12, 14, 16, 18** will acquire the information they need after one or more attempts or they will give up in frustration and access a competitor's home page or make a telephone call directly to the company.

The system **9** of the present invention for providing an advanced, selectively tailored Internet interface is shown in FIG. 3. As shown, both the information users **12, 14, 16, 18** and the information providers **20, 22, 24, 26** are selectable and changeable entities; in contrast to the static entities that presently comprise the Internet. As shown, the information user **12, 14, 16, 18** may tailor their information user profile as needed to acquire specific information. In this manner, one might even view the information user **12, 14, 16, 18** as having "multiple personalities."

As shown in FIG. 4A, for example, the information user **12, 14, 16, 18** may have a business profile **200** which is specifically tailored toward the information user's **12, 14, 16, 18** business needs. The profile **200** comprises a file **202** having a plurality of fields **204** which hold data that the information user **12, 14, 16, 18** is male, Caucasian, fiscally conservative, politically conservative, is employed by a Fortune 500 company, is employed in a sales position, has an undergraduate degree in economics, speaks English and is a U.S. resident.

Alternatively, as shown in FIG. 4B, the information user's **12, 14, 16, 18** profile **220** for accessing the Internet for pleasure comprises a file **202** having a plurality of fields **204** which hold data that the information user **12, 14, 16, 18** is a male, Caucasian, college graduate, has a liberal arts degree, homosexual, speaks several languages, has an annual income of $70,000-$100,000 socially liberal and fiscally liberal. It should be noted that a data file **250** having a standard format as shown in FIG. 4C may be adopted by all information users **12, 14, 16, 18** and information providers **20, 22, 24, 26** on the Internet. In this manner, a user may simply check or fill-in any of those user profile attributes **252A-252N** that are applicable. As shown, there are almost an unlimited number of columns which may be created to identify all of a user's attributes **252**. Additionally, a plurality of profiles **260A-260N** may be created by the user. For example, the user may create a business profile **260A** for all of his or her business trades, and then create several personal profiles **260B, 260C** for their personal traits. This profile is stored in computer memory (not shown) and transferred to an information provider **20, 22, 24, 26** when a Web page is accessed. These multiple profiles **252A-252N** are not unlike the multiple personalities that currently exist in every day life for many individuals. In accordance with the teachings of the present invention, the profiles **252A-252N** are selectively tailored to the needs of the information user **12, 14, 16, 18** at a particular time. Although several current Web pages permit a user to create a profile for that particular Web page, the information user **12, 14, 16, 18** must create this rudimentary profile each time they access the Web page. The present invention has the advantage that a detailed standard profile **252** may be created having an tremendous amount of detail and selectivity then this profile **252** may be utilized with any information provider that accepts the standard format.

Referring to FIG. 5A, an information provider **300** in accordance with the present invention is shown. The information provider **300** is a virtual panoply of information which is placed in a mosaic most pleasing to the information users **12, 14, 16, 18**. The information on the Web page **302** may be thought of as a mosaic of electronic tiles A, B, C1-C16, D, E, F, G each of which have a portion of the Web page **302**. Each tile A-G is a result of a separate data stream **310-322** which individually updates the tiles A-G. The tiles A-G may change, and the format and location of the data streams A-G may change as a result of the change in the data streams. As shown, the tiles A-G may be changed on a yearly, quarterly, daily, hourly or constant basis. Additionally, as shown, the entire Web page **302** may be changed, or only one or more portions of the Web page **302** may be changed as will be explained in detail hereinafter.

Each data stream **310-322** has a set of information identifiers for identifying the type of information provided by the data stream **310-322**. For example, the data stream **310** which supplies section A may carry general information regarding the Web page's owner such as a corporation. The file structure of the information identifiers **340A-340N** is shown in FIG. 5B. Among the plurality of other data streams **312-324** may exist intellectual property information such as a company's copyright and trademark notifications (section G) **318**; directions on how to reach the corporation's headquarters (section F) **320**, sales or service locations (section E) **322**; and a plurality of other information related to a company's products or services (sections B, C, D and H) **323, 314, 324, 312**. It should be apparent even to those with rudimentary skills in the art that the foregoing discussion regarding the data streams **310-324** involving a company's products or services may apply equally to any of the other data streams that are set forth on a Web page **300**.

The tailoring of a company's information or services will now be explained in detail hereinafter. The three data streams that will be selected are a company's logo (section H) **312**, a company's product line (section D) **324** and the description of the product line (section B) **323**. Although some of the data streams may be individually linked, such as a product and the description of the product and the price of the product; they will be treated separately for simplification of the explanation.

Tailoring of the data stream 312 of the company's logo will now be described. As shown in FIG. 6, this or any other data stream 310-324 may be tailored toward the time of day. This will give the information user 12, 14, 16, 18 the pleasing experience that the Web page 302 is "fresh." For example as shown in FIG. 6A, the logo H may be profiled by a rising sun during the early morning hours, a bright sun during the day and a setting sun in the late afternoon and early evening hours. The moon and stars may come out after nightfall, as shown in FIG. 6B, and would be an indication of the actual time of day. Although this may appear as a gimmick, the information user 12, 14, 16, 18 may access the Web page 302 all day long without actually seeing the same Web page 302 twice. It should be recognized that other portions of the Web page 302 may be likewise tailored. This could also be a powerful marketing concept whereby the logo might change color for a certain period of time indicating that the company's products are on sale, the stock is doing well or that the company is hiring. Any aspect of the logo H may be changed to provide useful information to the information user 12, 14, 16, 18. Additionally depending upon the profile 252 of the information the users 12, 14, 16, 18, a Japanese resident accessing a Web page may view a "sun rising" page, while simultaneously a U.S. resident will see the moon, stars and nightcap. The profile 252 will be downloaded to the information provider 20, 22, 24, 26.

Referring back to FIG. 5A, the data stream 323 concerning a company's products B will now be described in detail hereinafter. This data stream 323 is shown in greater detail in FIG. 7. As shown, the data stream 323 may comprise a plurality of separate data streams 323A-323C which change on a basis set by the information provider 20, 22, 24, 26. The first data stream 323A, for example, pertains to a company's "high end" line of products 380, the second data stream 323B may comprise a company's "middle end" line of products 382, and the third data stream 323C may comprise the company's "low end" line of products 384.

Each particular data stream 323A-323C may comprise the same products throughout the day as shown in FIG. 7, or may change periodically throughout the day, or based upon the time of day. For example, the high end line of products 380 may relate to gourmet coffee; the middle end line of products may relate to your average "cup of joe" 382; and the third data stream 323C may relate to your "get it hot" coffee line for people who are looking only for a caffeine intake and are willing to "choke down" any sludge 384. These three lines of products 380-384 may be displayed until approximately 11:00 a.m. Thereafter, three new high, middle and low end lines of products 380-384 are described such as a company's soda or tea beverage line. In the evening, the three data streams 323A-323C may again change to liquors used for after dinner drinks.

Referring to the high end product description data stream 323A, this data stream 323A may be selectively tailored in a different manner as will be described in detail hereinafter. For example, the data stream 323A may actually comprise three separate lines of data 323A1, 323A2, 323A3, one tailored towards very conservative, serious or older individuals 323A1, one tailored towards "no frills" type people who seek only raw data regarding a product, such as health conscious individuals 323A2; and a third data stream that is playful, light and funny for the common Internet surfer 323A3. Accordingly, going along with the present example the high end line of coffee products may be described in the conservative data stream as "a succulent blend of Columbian and Arabica beans which are blended for an exquisite taste and are dry roasted to relieve the coffee of any bitterness." This type

of explanation is specifically tailored to "high income and high end serious and conservative individuals who are looking for a premium product." The description of the high end product for the "data seeking" type of individual may read as follows "a blend of 60% Arabica, 40% Columbian coffee beans is blended and freeze dried at minus 60 degrees Celsius. A six ounce cup contains 100 calories, zero grams of fat . . . " For those generation X'ers who are accustomed to a "loud" advertising style, the following will suffice: "Yo! This cup of joe will be blow you away. Be the first of your friends to drink this liquid gold and have the bragging rights that you, truly, have it together." As can be seen by these differing descriptions, a conservative individual would clearly be turned off by the in-your-face manner of the third data stream. Likewise, younger individuals would most likely be bored by the first description. In this manner, a company can cater to all needs without having to boil down and sanitize a particular Web page to meet a majority market, while alienating minorities.

The most beneficial aspect of the present invention which permits a company to tailor the delivery of information to a specific user without requiring the user to input a lot of mundane and unnecessary information will now be described in detail. When an individual accesses a particular Web page, the individual's current profile that the individual has selected, (for example 252A), is automatically downloaded to that Web page. The Web page manager matches the user's profile to the information identifier's 340A-340N. Depending upon the number of matches, the manager selects the data stream that corresponds most closely with the profile 252A. In this manner, the Web page manager tailors the Web page to the specific individual based on the profile. The Web page manager selects most appropriate data streams for the current information user 12, 14, 16, 18 depending upon the currently available data streams and the profile of the individual. Although there may be a standard Internet protocol developed which may require an information user 12, 14, 16, 18 to input their profile in a standard format such as 100 different sorting aspects, this is not required. The Web page manager will use those downloaded portions and will tailor the Web page accordingly.

This system allows the information provider to selectively provide information to the information user without the information user's knowledge or without irking the information user by telling them they need a password, or they need to be a member. It permits those members to get to the information seamlessly. For example, low end users may receive coupons, high end users may receive product warranty information Another feature of the present invention is that it includes the ability to access a web site and map the entire web site. For example, as shown in FIG. 2, when an information user selects choice 1 Ai, the person does not know what exists in choice 1 Ci until they get there. Often, the person forgets the other choices available. The present invention may either map the route which the person has gone and provide a tree and branch diagram as a picture-in-picture window within the screen or may map the entire web site upon accessing the Web page. For example, when a person access a web site, the web site navigator resident within the information user's browser may quickly go in and access every page of the web site. It will then summarize, and categorize the information in a concise manner and provide a branch and tree type map.

Although the invention has been described in part by making detailed reference to certain specific embodiments, such details is intended to be instructive rather than restrictive. It will be appreciated by those skilled in the art that many variations may be made in the structure and mode of operation without departing from the spirit and scope of the invention as disclosed in the teachings herein.

Although the features and elements of the present invention are described in the preferred embodiments in particular combinations, each feature or element can be used alone (without the other features and elements of the preferred embodiments) or in various combinations with or without other features and elements of the present invention.

Hereafter, a wireless transmit/receive unit (WTRU) includes but is not limited to a user equipment, mobile station, fixed or mobile subscriber unit, pager, or any other type of device capable of operating in a wireless environment. When referred to hereafter, a base station includes but is not limited to a Node-B, site controller, access point or any other type of interfacing device in a wireless environment.

What is claimed is:

1. A system for providing web pages accessed from a web site in a manner which presents the web pages tailored to an individual user, comprising:

an interactive interface configured to provide dynamic web site navigation data to the user, the interactive interface comprising:

a display depicting portions of the web site visited by the user as a function of the web site navigation data; and

a display depicting portions of the web site visited by the user as a function of the user's personal characteristics.

2. The system of claim 1, wherein the display depicting portions of the web site visited by the user includes a map depicting a route of web pages visited by the user.

3. The system of claim 1, wherein the display depicting portions of the web site visited by the user includes a map of web pages visited by the user, presented in a tree and branch diagram in combination with at least a portion of the entire web site accessible by the user.

4. The system of claim 1, wherein the display depicting portions of the web site visited by the user includes an indication of web pages visited by the user, presented as a picture-in-picture window within the display in combination with at least a portion of the entire web site accessible by the user.

5. The system of claim 1, wherein the interactive interface:

includes a data file generated from user activity based on user data transmitted in response in part to user selections of a plurality of user-selectable fields, each field describing a personal characteristic of the user; and

is configured to automatically transmit data corresponding to the user selections upon initially accessing the web pages, wherein an analysis of the user selections provides a selection of a plurality of discrete web pages specifically tailored to the user; and the display depicting portions of the web site visited by the user includes data derived from at least one of the user data and user activity based on the user data.

6. The system of claim 1, wherein the interactive interface is further configured to generate a site map according to at least one of a route which the user has taken or a plurality of discrete sections tailored for the user, thereby providing a diagram in accordance with the user selections.

7. A method of generating a web page comprising:

generating a plurality of data streams, wherein each data stream is associated with a particular portion of the web page, and wherein each data stream is stored in a computer memory; and

changing at least one of the particular portions of the web page as a function of time.

8. The method of claim 7, wherein one of the particular portions presents a company logo, wherein the company logo is profiled by different symbols depending upon the time of day.

9. The method of claim 7, wherein the different symbols indicate the time of day.

10. The method of claim 7, wherein at least a part of one of the particular portions presents information associated with a company, wherein the at least part of one of the particular portions changes color for a certain period of time to indicate an event or condition associated with the company.

11. The method of claim 7, wherein the event or condition is associated with the price of products sold by the company.

12. The method of claim 7, wherein the event or condition is associated with the type of products sold by the company.

13. The method of claim 7, wherein the event or condition is associated with the price of stock associated with the company.

14. The method of claim 7, wherein the event or condition is associated with employment opportunities offered by the company.

15. The method of claim 7, wherein the particular portions present different products at different times during each day.

16. A method comprising:

receiving data which defines a plurality of user profile attributes in each of a plurality of user profiles;

storing the plurality of user profiles, each user profile comprising data descriptive of a user;

in response to a request from an information provider, transferring data from a specified user profile to the information provider; and

providing dynamic web site navigation data via an interactive interface, the interactive interface comprising:

a display depicting portions of a web site visited by the user as a function of web site navigation data; and

a display depicting portions of a web site visited by the user as a function of the plurality of fields having data descriptive of a user.

17. The method of claim 16, further comprising: transferring the stored plurality of user profiles to an information provider when a web page is accessed.

18. The method of claim 16, wherein data from the plurality of profiles are transferred in a standardized form.

19. The method of claim 16, wherein the plurality of user profiles include at least one of a business profile, a personal profile, and a family profile.

20. The method of claim 16, wherein the profile attributes include at least one of gender, race, income, and education.

21. A method comprising:

receiving data from a user profile associated with a user;

in response to a request associated with the user, sending a data stream that is selected based at least in part on the received data from the user profile; and

displaying the data stream via an interactive interface, the interactive interface comprising:

a display depicting portions of a web site visited by the user as a function of web site navigation data; and

a display depicting portions of a web site visited by the user based at least in part on the received data from the user profile.

22. The method of claim 21, further comprising:

selectively offering a coupon to the user associated with the request, wherein the coupon is based at least in part on the received data from the user profile.

23. The method of claim 21, further comprising:

selectively presenting product warranty information to the user associated with the request, wherein the product warranty information is based at least in part on the received data from the user profile.

* * * * *

US006182894B1

(12) **United States Patent**
Hackett et al.

(10) **Patent No.: US 6,182,894 B1**
(45) **Date of Patent: Feb. 6, 2001**

(54) **SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION CARD**

(75) Inventors: **Ann Hackett**, Phoenix; **Lisa Arnold**, Glendale; **Vickie Jordan**, Phoenix, all of AZ (US)

(73) Assignee: **American Express Travel Related Services Company, Inc.**, New York, NY (US)

(*) Notice: Under 35 U.S.C. 154(b), the term of this patent shall be extended for 0 days.

(21) Appl. No.: **09/181,734**

(22) Filed: **Oct. 28, 1998**

(51) **Int. Cl.**^{7} **G06K 5/00**
(52) **U.S. Cl.** **235/380**; 235/382.5
(58) **Field of Search** 235/380, 375, 235/382, 382.5, 379; 380/23

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,643,453		2/1987	Shapiro et al. .	
4,734,568		3/1988	Watanabe .	
4,798,403		1/1989	Nelson .	
4,831,245		5/1989	Ogasawara .	
4,837,422	*	6/1989	Dethloff et al.	235/380
4,947,027		8/1990	Golightly .	
4,998,279	*	3/1991	Weiss	380/23
5,168,520	*	12/1992	Weiss	380/23
5,239,538	*	8/1993	Tell, Jr. et al.	370/58.3
5,251,259	*	10/1993	Mosley	380/23
5,259,649		11/1993	Shomron .	
5,276,314	*	1/1994	Martino et al.	235/380
5,341,428	*	8/1994	Schatz	380/23
5,343,529	*	8/1994	Goldfine et al.	380/23
5,400,082		3/1995	Kamiya .	
5,615,277	*	3/1997	Hoffman	382/115
5,617,470		4/1997	DePasquale .	
5,627,355		5/1997	Rahman et al. .	
5,742,035		4/1998	Kohut .	

OTHER PUBLICATIONS

Shaughnessy, John, Vice President, Fraud Reduction Programs, "Authorization Message Will Be Adapted to Accommodate Card Verification value 2 Processing", Feb. 1998, Visa Net Processor Digest, pp. 6–7.

* cited by examiner

Primary Examiner—Thien M. Le
(74) *Attorney, Agent, or Firm*—Snell & Wilmer L.L.P.

(57) **ABSTRACT**

Instead of a PIN which is associated with an account and provides access to an account, a card identification code, which is located on the card but does not provide automatic access to an account, is used to verify that the consumer currently possesses the transaction card at the time of purchase and/or is the true card owner. At the time of card printing, an embossing file of account codes including associated identification codes is created and loaded into the account database. At the time of authorization, the identification code and the account code are entered into a POS device and sent to an authorization system. If the identification codes match, and other authorization parameters are satisfied, the transaction card is authorized.

18 Claims, 5 Drawing Sheets

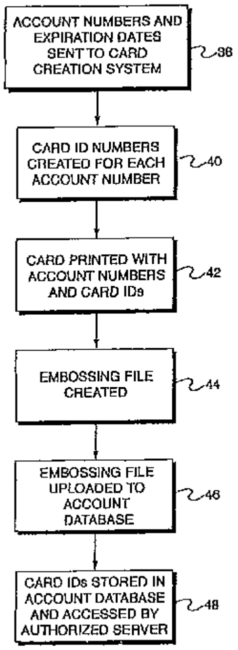

ACCOUNT NUMBERS AND EXPIRATION DATES SENT TO CARD CREATION SYSTEM
38
CARD ID NUMBERS CREATED FOR EACH ACCOUNT NUMBER
40
CARD PRINTED WITH ACCOUNT NUMBERS AND CARD IDs
42
EMBOSSING FILE CREATED
44
EMBOSSING FILE UPLOADED TO ACCOUNT DATABASE
46
CARD IDs STORED IN ACCOUNT DATABASE AND ACCESSED BY AUTHORIZED SERVER
48

EXHIBIT
"C"

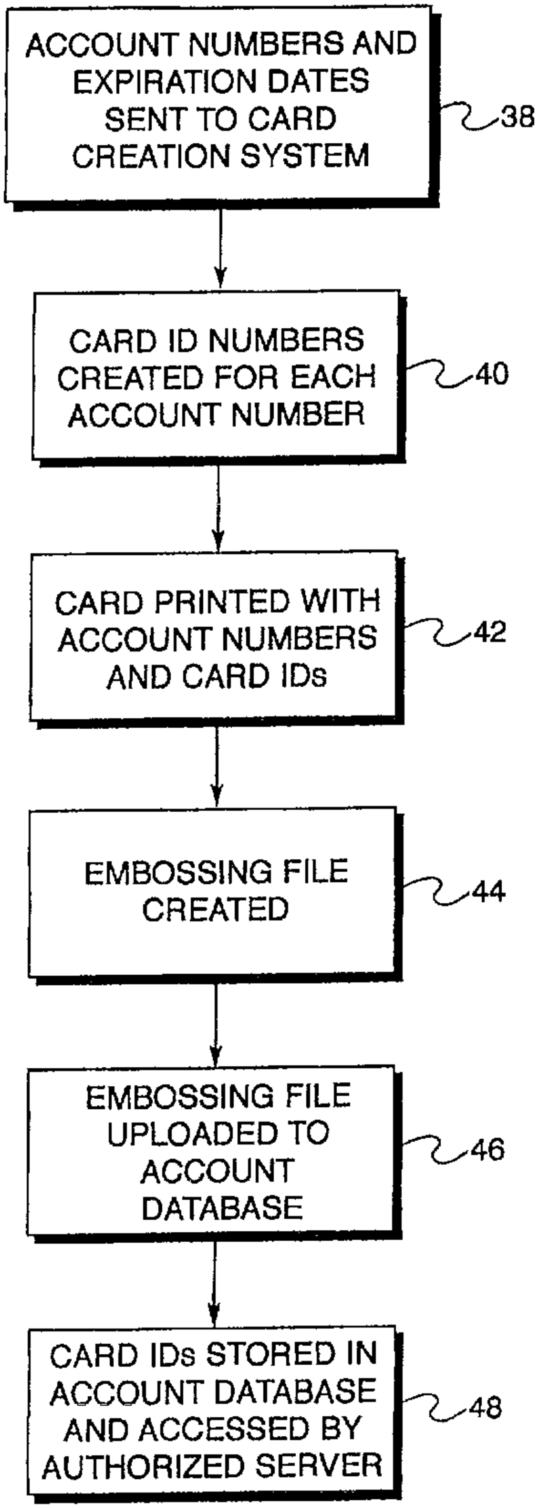

ACCOUNT NUMBERS AND EXPIRATION DATES SENT TO CARD CREATION SYSTEM
38
CARD ID NUMBERS CREATED FOR EACH ACCOUNT NUMBER
40
CARD PRINTED WITH ACCOUNT NUMBERS AND CARD IDs
42
EMBOSSING FILE CREATED
44
EMBOSSING FILE UPLOADED TO ACCOUNT DATABASE
46
CARD IDs STORED IN ACCOUNT DATABASE AND ACCESSED BY AUTHORIZED SERVER
48

FIG. 1.

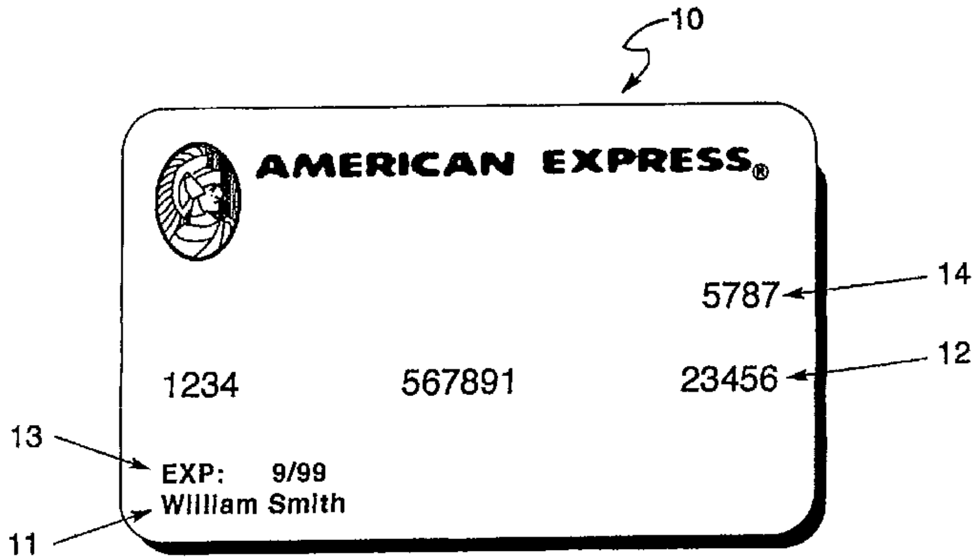

10
AMERICAN EXPRESS®
5787
14
1234
567891
23456
12
13
EXP: 9/99
William Smith
11

FIG. 2A.

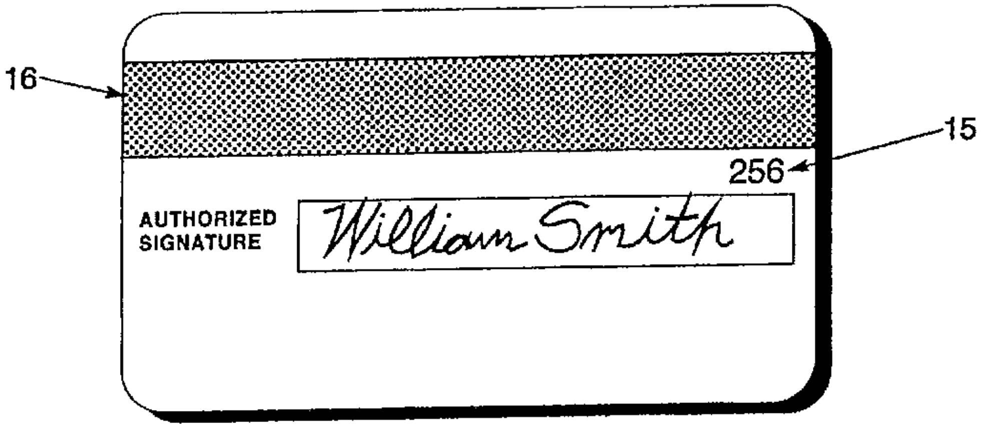

16
15
256
AUTHORIZED SIGNATURE
William Smith

FIG. 2B.

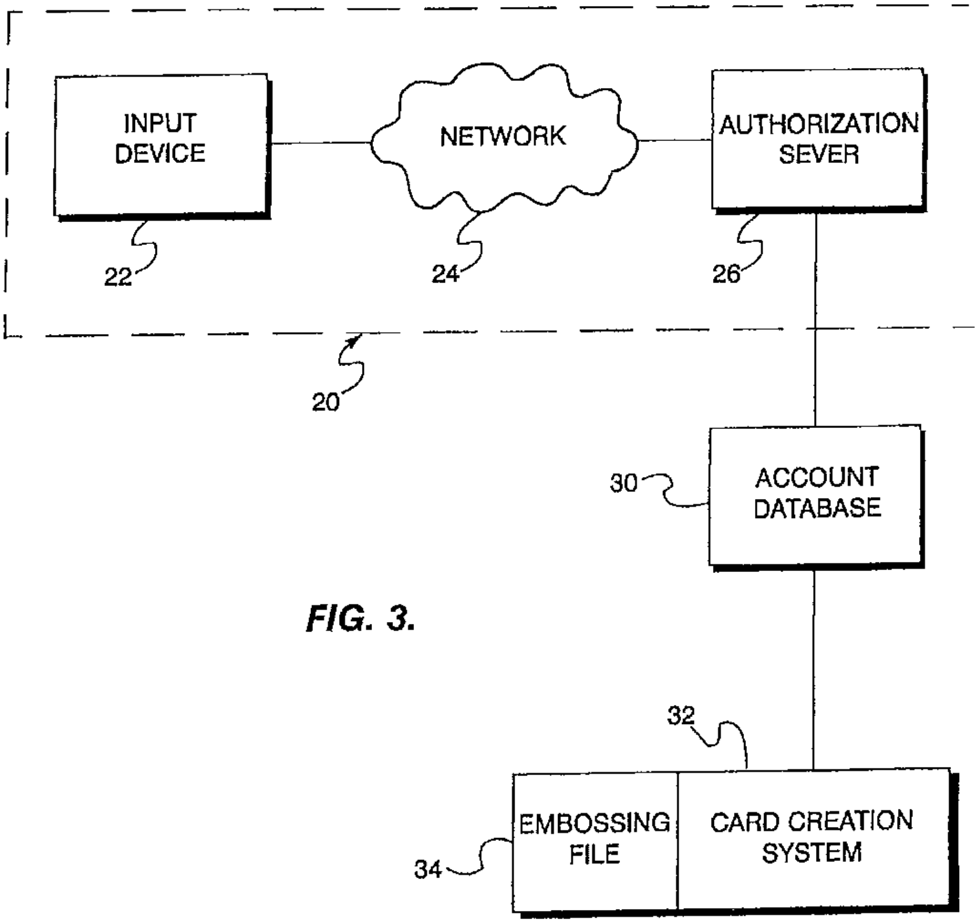
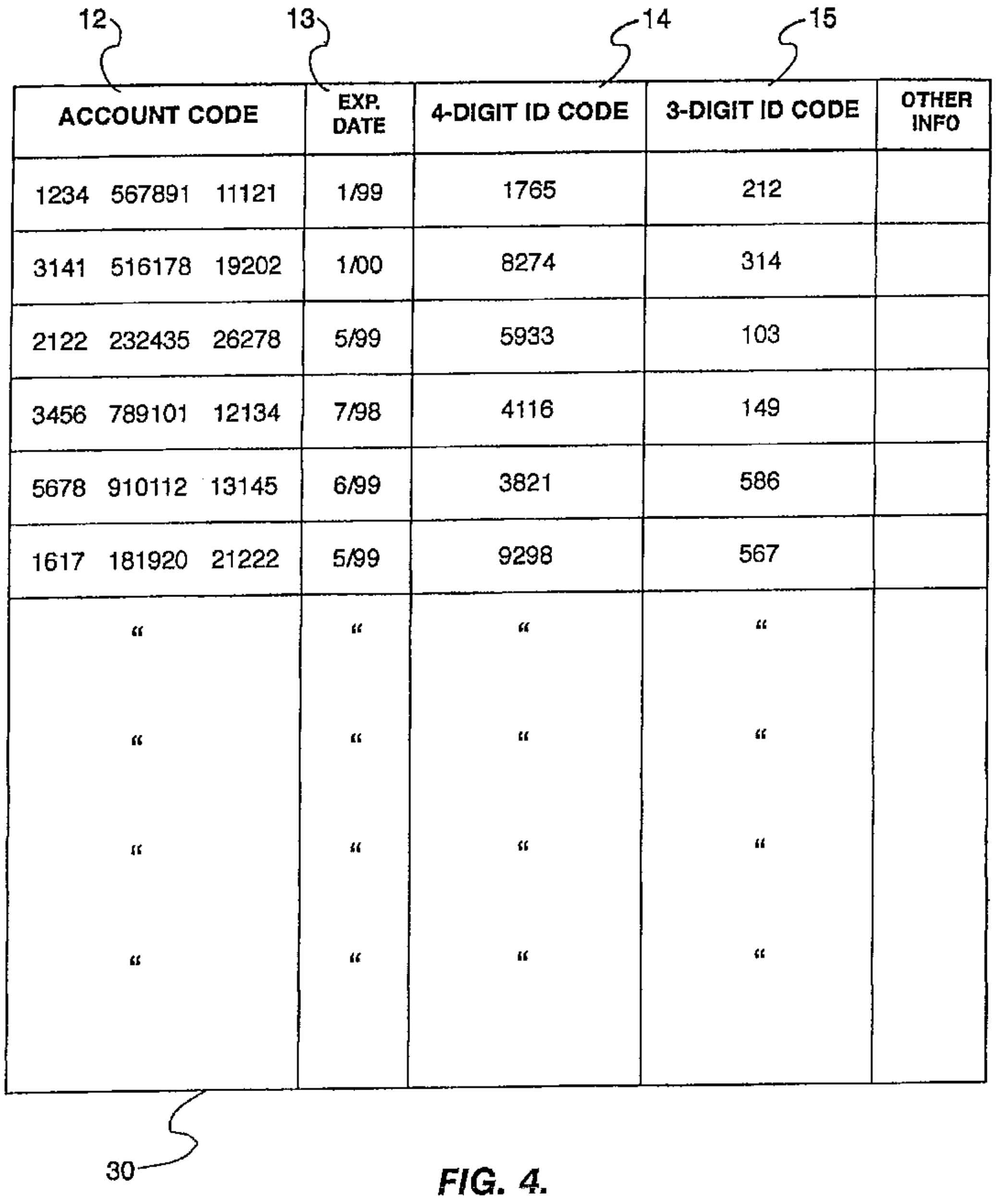

INPUT DEVICE
NETWORK
AUTHORIZATION SEVER
22
24
26
20
30
ACCOUNT DATABASE
32
EMBOSSING FILE
CARD CREATION SYSTEM
34

FIG. 3.


12
13
14
15
30

ACCOUNT CODE	EXP. DATE	4-DIGIT ID CODE	3-DIGIT ID CODE	OTHER INFO
1234 567891 11121	1/99	1765	212	
3141 516178 19202	1/00	8274	314	
2122 232435 26278	5/99	5933	103	
3456 789101 12134	7/98	4116	149	
5678 910112 13145	6/99	3821	586	
1617 181920 21222	5/99	9298	567	
"	"	"	"	
"	"	"	"	
"	"	"	"	
"	"	"	"	

FIG. 4.

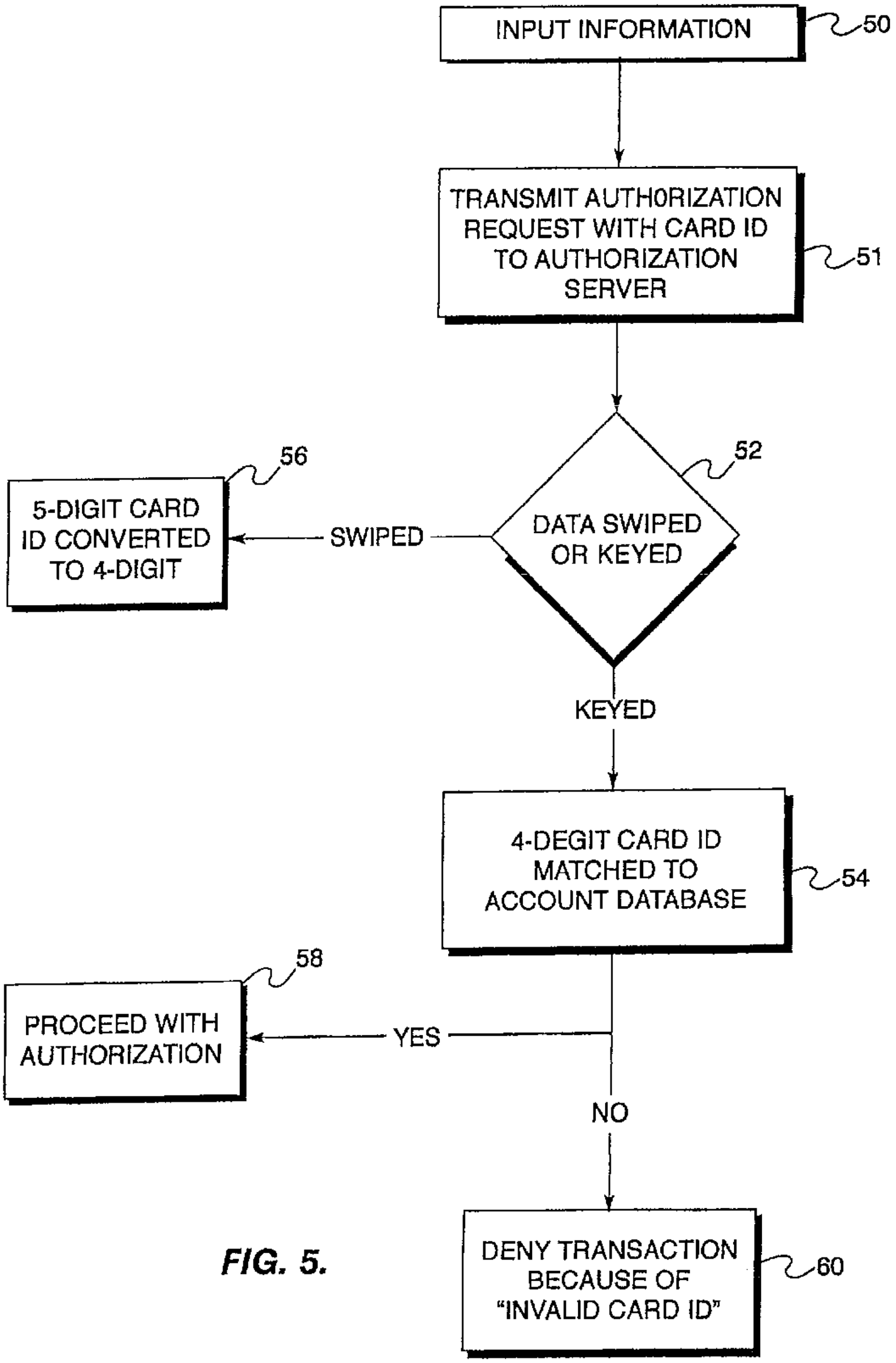

INPUT INFORMATION
50
TRANSMIT AUTH0RIZATION REQUEST WITH CARD ID TO AUTHORIZATION SERVER
51
DATA SWIPED OR KEYED
52
SWIPED
5-DIGIT CARD ID CONVERTED TO 4-DIGIT
56
KEYED
4-DEGIT CARD ID MATCHED TO ACCOUNT DATABASE
54
YES
PROCEED WITH AUTHORIZATION
58
NO
DENY TRANSACTION BECAUSE OF "INVALID CARD ID"
60

FIG. 5.

SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION CARD

BACKGROUND OF THE INVENTION

1. Technical Field

The present invention relates, generally, to transaction card fraud reduction systems and methods and, more particularly, to verifying that a consumer is in possession of a transaction card and/or is the true card owner during a purchase transaction.

2. Background Information

Transaction cards such as, for example, credit cards, debit cards, bank cards, charge cards, smart cards and the like, have become increasingly popular for purchasing goods and services and for conducting other transactions. A transaction card typically includes information related to the issuer's name and logo, an account number, an expiration date and the cardholder's name. The cards may also have other information, serial number and/or the like printed on the card to represent other information about the transaction card or about the card member such as, for example, a group number, a promotion number, a card type number, a plastic issuance number and/or the like. Certain information is often embossed on the card with raised print, thereby allowing the information to be imprinted on a charge slip; however, the information that is unembossed (flat) would not be imprinted onto the charge slip. For many transaction cards, the information printed on the card is also contained within a magnetic stripe, a bar code and/or an integrated circuit (microchip) for automatic downloading/reading by a card reader.

Many card transactions are commenced by inserting, or sliding a card through, a card reader which automatically downloads the card information, thereby allowing the information to be used during the authorization process without the need for manual input or review of the card information. However, because of the substantial increase in fraudulent use and theft of transaction cards, the use of the card information is often supplemented by various fraud prevention techniques, such as requiring a signature to verify the consumer's agreement to the transaction or the entry of a PIN number to verify the consumer's authority to use the transaction card.

Additionally, certain card issuers, such as banks, incorporate the consumer's picture onto the face of the transaction card to give the merchant an additional verification procedure.

While the use of a signature, PIN or picture is effective for fraud reduction when the cardholder presents a card to a merchant, these options are not as effective, and may not be available, for other transactions. Particularly, transactions which do not require face-to-face contact between a consumer and merchant, such as the use of a transaction card to purchase items through the Internet or over the telephone (e.g., mail order). Moreover, many transactions may be alternatively completed without using the physical transaction card. For example, a consumer or merchant may simply key in the transaction card number into the keypad of a POS device or the keypad on an ATM.

When conducting Internet, telephone or keypad transactions, a cardholder may only need to provide a card account number and expiration date to allow the merchant to charge a particular account and verify that the transaction card is valid. Other verification information, such as a PIN number, is usually not disclosed because the PIN is typically memorized by the cardholder and never disclosed to anyone. Because merchants often only request limited information to conduct a transaction over the Internet or the telephone, an increased potential for fraud exists due to the increased availability of this general information. In other words, regardless of a consumer's possession of the physical transaction card, a consumer can still fraudulently obtain and provide this general information.

Particularly, cardholders often provide a transaction card number to telemarketers, merchants, bank tellers and Internet sites, thereby allowing a merchant or clerk to retain the credit card number and associated information for later fraudulent use. Moreover, a person may overhear a transaction card number being disclosed over the telephone or, with the increase of mailbox thefts, a person may obtain a credit card number from a billing statement or promotional literature. Furthermore, advanced computer operators are able to intercept transaction card numbers which are transmitted over modems and/or the Internet. Accordingly, when a merchant simply requests a credit card number from a consumer, it is difficult for the merchant to ensure that the consumer placing the order has the transaction card in his or her possession and/or is the true cardmember, rather than using a stolen account number.

As stated above, the use of PIN numbers are typically limited to face-to-face or ATM transactions wherein the consumer personally enters a PIN into a keypad and the merchant does not need to have knowledge of the PIN. In non face-to-face transactions, the PIN would need to be disclosed to the merchant. However, due to security concerns, consumers prefer to not disclose their private PIN number to merchants and especially prefer to not disclose the PIN number over a telephone or through the Internet. Particularly, a PIN number is directly associated with the account number, and as such, may provide increased access to a transaction card account during a fraudulent transaction. Accordingly, a system is needed which allows the consumer to disclose a security number which is associated with the account number, but does not allow automatic access to the account.

BRIEF SUMMARY OF THE INVENTION

Due to security concerns during non face-to-face commercial transactions, consumers prefer to not disclose their private PIN number to merchants and especially prefer to not disclose the PIN numbers over a telephone or through the internet. Instead of a PIN which is associated with an account and provides access to an account, a card identification code, which is located on the card but does not provide automatic access to an account, is used to verify that the consumer currently possesses the transaction card at the time of purchase and/or is the true card owner.

Along with the account number, a transaction card includes a non-embossed four-digit or three-digit number, called a card identification code. During creation of a transaction card, a five-digit identification code is calculated from the account number, four-digit or three-digit identification code and the expiration date based upon a predetermined algorithm. A four-digit identification code is printed on the front of the card, an associated five-digit identification code is entered into the magnetic stripe and an associated three-digit identification code is printed in the signature panel. An embossing file of account numbers including associated identification codes is created and loaded into the account database. At the time of authorization, the four-digit number on the front of the card and the account number are manually keyed into a POS device and sent to an authorization system. The four-digit number is matched to the four-digit number on file for that transaction card. If the four-digit numbers match, and other authorization parameters are satisfied, the transaction card is authorized.

Alternatively, when the card is swiped through a POS device, the five-digit number previously entered into the magnetic stripe, along with other information, is automatically transmitted to the authorization system. The five-digit number is decomposed using a mathematical algorithm, and the resulting three-digit and/or four-digit numbers are matched against the database record (which includes the originally assigned three or four-digit identification codes for the account number). If the respective three or four-digit numbers match, and other authorization parameters are satisfied, the transaction card is authorized.

Thus, the entry of an additional identification code helps verify that the consumer currently possesses the transaction card at the time of purchase or is the true card owner, rather than simply using a stolen account number. Accordingly, requiring entry of an identification code along with the account number provides an effective deterrent to fraudulent use of the account number. For example, systems and methods in accordance with the present invention at certain tested locations have provided fraud reduction of approximately 78%.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

The subject invention will hereinafter be described in conjunction with the appended drawing figures, wherein like numerals denote like elements, and:

FIG. 1 is an exemplary flow diagram of the card creation and identification code creation process;

FIG. 2*a* is a front view of an exemplary transaction card showing an account number and card identification code;

FIG. 2*b* is a rear view of an exemplary transaction card showing magnetic strip and card identification code;

FIG. 3 is an exemplary schematic diagram of a simplified transaction card authorization system;

FIG. 4 is an exemplary schematic diagram of an authorization database with associated identification codes in accordance with an embodiment of the present invention; and,

FIG. 5 is an exemplary flow diagram of the authorization process.

DETAILED DESCRIPTION OF THE INVENTION

To reduce fraud when conducting commercial transactions (i.e., the purchase of goods and services) using a transaction card 10, the present system requests entry of an additional number to help verify that the consumer has possession of the transaction card at the time of purchase or is the true card owner, rather than simply using a stolen account code. Wherein a PIN number is typically memorized and not written down, the present number, called a card identification code 14, 15 and 16, is preferably printed on or encoded in transaction card 10. Due to security concerns during non face-to-face transactions, consumers prefer to not disclose their private PIN number to merchants and especially prefer to not disclose the PIN number over a telephone or through the Internet. Instead of a PIN which is associated with an account and provides access to an account, a card identification code 14, 15 and 16, which does not provide automatic access to an account, is used to help verify that the consumer currently possesses the transaction card at the time of purchase and/or is the true card owner.

With momentary reference to FIG. 2*a*, in accordance with the present invention, a transaction card 10 includes any device suitably configured to display an account code 12 and a card identification code 14. In a preferred embodiment, the transaction card is a credit card, charge card, debit card, smart card, bank card and/or the like. Transaction card 10 preferably includes information for conducting a transaction. In a preferred embodiment, the front face of transaction card 10 includes an account code 12 and a card identification code 14 located above account code 12. Account code 12 includes any number of characters (n characters) comprising any combination of numbers, letters, symbols or other indicia which are suitably configured to identify a transaction account. In a preferred embodiment, account code 12 is a 15-digit number which identifies an account code, including a routing number or other similar transaction numbers, corresponding to the card owner. One of ordinary skill in the art will appreciate that account code 12 may be associated with an individual account, a corporate account, an organization account, or any other entity and the account may represent a charge account, a credit account, a debit account, an electronic purse account, or any other financial account.

Card identification codes 14, 15 and 16 include any number of characters (n characters) comprising any combination of numbers, symbols, letters, or other indicia suitably configured to provide verification that the consumer has an actual card in possession at the time of purchase and/or is the true card owner, rather than simply using a stolen account code. In a preferred embodiment, card identification code 14 is printed on or encoded in transaction card 10. Card identification code 14 may be located on either side of the card, encoded into a medium on the card and may be embossed (raised lettering) or unembossed (flat) into the plane of the card. In a particularly preferred embodiment, card identification code 14 is located on the front face of transaction card 10 on the same side as, and above, account code 12. Moreover, card identification code 14 is preferably a four-digit, unembossed (flat) number printed within the plane of the card. One skilled in the art will appreciate that, along with other card member information, card identification codes 14, 15 or 16 may be initially printed on many transaction cards 10 before, during or after account code 12 is printed on transaction card 10. In a preferred embodiment, card identification codes 14 or 15 are logically related to card identification code 16.

After a consumer is approved for a transaction card, an account code 12, a four-digit identification code 14 and/or a three digit code 15, an expiration date 13 and other information are associated with the consumer's name in an account database 30 (see FIGS. 2*a* and 3). With reference to FIGS. 1 and 3, account code 12, a four-digit identification code 14 (or a three-digit identification code 15), an expiration date 13 and other information from account database 30 are preferably transmitted to a card creation system 32 (step 38). In a preferred embodiment, at the time of creating transaction card 10 for the consumer in accordance with the present invention, a five-digit identification code 16 is suitably calculated from account code 12, four-digit identification code 14 or three-digit identification code 15 and expiration date 13 based upon a predetermined algorithm (step 40). Five-digit identification code 16 is preferably calculated and encoded into the magnetic stripe because five-digit identification code 16 provides additional security by not being disclosed on the face of the card (only four-digit code 14 or three-digit code 15 are visible).

After determining identification codes 14, 15 and 16, transaction card 10 is preferably created with an embossed account code 12, embossed expiration date 13, embossed consumer's name 11 and non-embossed card identification codes 14, 15 and 16 (step 42). Particularly, in a preferred embodiment, a four-digit identification code 14 is printed (non-embossed) on the front of card 10 above account code 12, an associated five-digit identification code 16 is encoded into the magnetic stripe and an associated three-digit identification code 15 is printed in the signature panel. One skilled in the art will appreciate that any one of the aforementioned card identification codes 14, 15 and 16 may exist throughout this process alone or in any combination with the other card identification codes. For example, only identification code 14 may appear on the front of the card without any codes on the back of the card or in the magnetic stripe. Moreover, identification codes 14, 15 and 16 may comprise any number of digits, symbols, characters, letters and/or the like and may be located in any location and in any medium on card 10. For example, an identification code may be encoded into an integrated circuit in a smart card embodiment.

Upon printing of transaction cards 10, an embossing file 34 including card identification codes 14, 15 and 16 is created (step 44). Embossing file 34 with associated identification codes 14, 15 and 16 is next uploaded into account database 30 (step 46). In a preferred embodiment, authorization server 26 communicates with, and analyzes the data within, account database 30 (step 48). Alternatively, the use of a Hardware Security Module allows embossing file 34 to provide a simplified, more direct transmission of embossing information to account database 30 without the need for maintenance uploads. In a particularly preferred embodiment, as shown in FIG. 4, identification codes are stored in a look-up table within account database 30.

Referring to FIG. 3, an exemplary authorization system 20, account database 30 and card creation system 32 is shown. Authorization system 20 is any authorization system suitably configured to authorize a transaction card and notify an input device 22 of the authorization status. One skilled in the art will appreciate that authorization system 20 can be an existing authorization system, such as the Central Authorization System used by American Express, which is re-programed or re-configured to preform the functions of the present invention or is a system specially configured to preform the functions of the present invention. In a preferred embodiment, authorization system 20 includes input device 22, network 24 and authorization server 26. input device 22 is any device suitably configured to accept transaction information and transmit the information for approval. In a preferred embodiment, input device 22 is a telephone, computer, point-of-sale terminal, ATM and/or the like. Input device 22 preferably communicates with network 24, wherein network 24 is any device or software suitably configured to transmit information. In a preferred embodiment, network 24 is a modem, a PSTN, an Internet, an Intranet, a direct link, or any combination thereof.

With continued reference to FIG. 3, network 24 provides a communication link between input device 22 and authorization server 26. Authorization server 26 is any device suitably configured to authorize a transaction and/or transaction card and notify input device 22 of the authorization status. In a preferred embodiment, authorization server 26 is a centralized authorization system including transaction account codes. One skilled in the art will appreciate that authorization server 26 can be a centralized database providing authorization information to various input devices 22. Moreover, one skilled in the art will appreciate that authorization server 26 may include any combination of components, software, servers and computers suitably configured to not only authorize transactions and/or transaction cards, but also to provide additional transaction support such as report generation and promotional programs. Authorization server 26 is preferably in communication with, and interrogates, account database 30. One skilled in the art will appreciate that account database 30 can be a separate component, integrated into authorization server 26 or simply software within authorization server 26 or within input device 22. In a preferred embodiment, account database 30 includes a look-up table (see FIG. 4), thereby allowing verification of the association between account codes 12 and identification codes 14, 15 and 16.

Referring to FIG. 5, when a consumer uses transaction card 10, a clerk, sales representative, merchant, consumer or other authorized person inputs account code 12 and card identification code 14, 15 or 16, along with any other transaction information such as purchase amount, etc., into input device 22 (step 50). In one embodiment, card identification code 14 or 15 is manually keyed into input device 22. The keyed information is sent via network 24 to authorization server 26 (step 25 51). Authorization server 26 suitably determines if the data was keyed in or swiped through input device 22 (step 52). In a preferred embodiment, to help determine if the data was keyed or swiped, the keyed data includes different formatting, uses different communication lines, different number of digits in the identification code and/or different header information than information read from the magnetic stripe.

After authorization server 26 determines that the information is manually keyed information, authorization server 26 suitably interrogates account database 30 to determine if the keyed identification code 14 or 15 matches the respective identification number on file for that transaction card (step 54). If the respective identification codes 14 or 15 match, the authorization process proceeds to determine if other authorization parameters are satisfied (step 58). If the respective identification codes 14 or 15 do not match, the transaction is denied and an "invalid Card ID" message is transmitted to the input device 22 (step 60). In an alternative embodiment, if the identification numbers do not correspond, authorization server 26 preferably prompts input device 22 to re-enter the card identification code and the process is repeated. If the numbers do not correspond again, transaction card 10 is denied.

When the card is swiped through a POS device 22, the five-digit number previously entered into the magnetic stripe, along with other information, is automatically transmitted to authorization server 26. Authorization server 26 suitably determines that the data originated from a magnetic stripe (step 52) by various methods such as, for example, data format, communication lines from which the data was sent, header information and/or the number of digits in the identification code. Authorization server 26 preferably decomposes the five-digit identification code 16 into a four-digit number using a predetermined mathematical algorithm (step 56). In a preferred embodiment, this algorithm is the inverse of the algorithm set forth above used to create the five-digit identification code 16. Alternatively, account database 30 includes five-digit identification codes 16 for each account code 12, thereby eliminating the need to transform the five-digit code 16 to a four-digit code 14. The algorithm is optimally a robust and secure algorithm which conforms to the Data Encryption Standard. Similar to above, authorization server 26 then suitably interrogates account database **30** to determine if the derived four-digit number **14** matches the four-digit number on file for that transaction card (step **54**). If the fourdigit numbers match, the authorization process proceeds to determine if other authorization parameters are satisfied (step **58**). If the four-digit numbers do not match, the transaction is denied and an "invalid Card ID" message is transmitted to the input device **22** (step **60**). In an alternative embodiment, if the numbers do not correspond, authorization server **26** preferably prompts input device **22** to re-swipe the card identification code **16** and the process is repeated. If the numbers do not correspond again, transaction card **10** is denied.

In a further alternative embodiment, the incorporation of card identification code **14** into a particular authorization process is optional depending on the type of transaction card **10** or account code **12** used for the financial transaction. In other words, when authorizing a transaction, the same authorization system **20** may not require a card identification code **14** for particular account codes **12**. For example, certain consumers may be enrolled in a promotional program which includes a cardless account without a card identification code **14**. As such, while other verification means typically exist, authorization server **26** may not require entry of an identification code or account database **30** may include any suitable automatic authorization for certain ranges of account codes **12**, regardless of entry of a card identification code **14**.

In a preferred embodiment, account codes **12** are subject to periodic update as new card promotions or new accounts are opened. For security reasons, card identification codes **14**, **15** or **16** are preferably only retained in authorization server **26** until authorization or rejection is received by input device **22**. Moreover, in a preferred embodiment, card identification codes **14**, **15** or **16** are not permanently stored in the input device **22** or the authorization server **26** and are not printed on documents (i.e., receipts, tickets, itineraries, etc.).

Although the invention has been described herein in conjunction with the appended drawings, those skilled in the art will appreciate that the scope of the invention is not so limited. Modifications in the selection, design and arrangement of various components and steps discussed herein may be made without departing from the scope of the invention as set forth in the claims. Moreover, the present invention may be described herein in terms of functional block components and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware components configured to perform the specified function. For example, the present invention may employ various integrated circuit components, e.g., memory elements, digital signal processing elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more micro-processors or other control devices.

In addition, those skilled in the art will appreciate that the present invention may be practiced in any number of data communication contacts and that the authorization system described herein is merely one exemplary application for the invention. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, training, signal processing and conditioning, and the like. Such general techniques that may be known to those skilled in the art are not described in detail herein.

We claim:

1. A system for authorizing commercial transactions comprising:

a transaction card having an n character account code and an n character identification code, wherein said identification code is not an expiration date and wherein said account code and said identification code have a predetermined logical relationship;

an input device for receiving said account code and said identification code; and,

an authorization computer in communication with said input device, said authorization computer configured to confirm said predetermined relationship between said account code and said identification code.

2. The system of claim **1**, wherein said transaction card is at least one of a credit card, debit card, bank card, charge card and smart card.

3. The system of claim **1**, where in said identification code is unembossed.

4. The system of claim **1**, wherein said account code and said identification code are on the same side of said transaction card.

5. The system of claim **1**, wherein said input device is at least one of a keypad, POS terminal, ATM terminal, computer and telephone.

6. The system of claim **1**, wherein said identification code is at least one of a three-digit number, four-digit number and five-digit number.

7. The system of claim **1**, wherein said account code and said identification code are on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.

8. The system of claim **1**, wherein said authorization computer is configured to transform said identification code to a second identification code.

9. The system of claim **1**, wherein said authorization computer communicates with an account database and said authorization computer is configured to confirm said predetermined relationship between said account code and said identification code by interrogation of said account database.

10. A method for obtaining an authorization for a commercial transaction comprising:

keying an n character account code and an n character identification code into an input device, wherein said identification code is not an expiration date and wherein said account code and said identification code have a predetermined logical relationship;

communicating, from said input device to an authorization computer, said account code and said identification code; and,

receiving a confirmation from said authorization computer of said predetermined relationship between said account code and said identification code.

11. The method of claim **10**, wherein said keying step includes keying said n character account code and said n character identification code into said input device, wherein said input device is at least one of a keypad, POS terminal, ATM terminal, computer and telephone.

12. The method of claim **10**, wherein said keying step includes keying said account code and said identification code which are located on a transaction card, further wherein said account code and said identification code are printed on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.

13. The method of claim **10**, further comprising transforming, via said authorization computer, said identification code to a second identification code.

14. The method of claim **10**, further comprising communicating between said authorization computer and an account database and confirming, via said authorization computer, said predetermined relationship between said account code and said identification code by interrogating said account database.

15. A transaction card for authorizing commercial transactions comprising:

an n character account code in a first field;

an n character identification code in a second field, wherein said identification code is not an expiration date;

wherein said account code and said identification code have a predetermined logical relationship;

said transaction card configured to provide, via an input device, said account code and said identification code to an authorization computer, wherein said authorization computer is configured to confirm said predetermined relationship between said account code and said identification code.

16. The system of claim 15, wherein said transaction card is at least one of a credit card, debit card, bank card, charge card and smart card.

17. The system of claim 15, wherein said account code and said identification code are on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.

18. At an authority responsible for authorizing a transaction, a computer-implemented method for handling an authorization request, comprising the following steps:

receiving an n character account code and an n character identification code from an input device, wherein said account code and said identification code have a predetermined logical relationship;

confirming said predetermined relationship between said account code and said identification code; and,

processing the authorization request.

* * * * *

US008083137B2

(12) **United States Patent**
Tannenbaum

(10) **Patent No.: US 8,083,137 B2**
(45) **Date of Patent: *Dec. 27, 2011**

(54) **ADMINISTRATION OF FINANCIAL ACCOUNTS**

(75) Inventor: **Mary C. Tannenbaum**, Dallas, TX (US)

(73) Assignee: **Niaco Data Mgmt. II, LLC**, Wilmington, DE (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 98 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/472,177**

(22) Filed: **May 26, 2009**

(65) **Prior Publication Data**

US 2009/0234766 A1 Sep. 17, 2009

Related U.S. Application Data

(60) Division of application No. 11/567,044, filed on Dec. 5, 2006, now Pat. No. 7,540,411, which is a division of application No. 10/192,426, filed on Jul. 10, 2002, now Pat. No. 7,254,548, application No. 12/472,177, which is a division of application No. 11/567,032, filed on Dec. 5, 2006, now Pat. No. 7,870,027, application No. 12/472,177, which is a division of application No. 11/767,246, filed on Jun. 22, 2007, which is a continuation-in-part of application No. 10/192,426, filed on Jul. 10, 2002, now Pat. No. 7,254,548, application No. 12/472,177, which is a division of application No. 11/567,069, filed on Dec. 5, 2006, which is a continuation of application No. 10/192,426, filed on Jul. 9, 2002, now Pat. No. 7,042,830.

(51) **Int. Cl.**
G06K 5/00 (2006.01)

(52) **U.S. Cl.** 235/380; 235/382

(58) **Field of Classification Search** 235/380, 235/382, 381, 382.5, 375, 492, 493
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,194,472	A	3/1993	Wilson et al.
5,444,616	A	8/1995	Nair et al.
5,513,272	A	4/1996	Bogosian, Jr. et al.
5,708,422	A	1/1998	Blonder et al.
5,764,789	A	6/1998	Pare et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0150428	7/2001

(Continued)

OTHER PUBLICATIONS

"Non Final Office Action", U.S. Appl. No. 11/767,246, (Jun. 25, 2009), 17 pages.

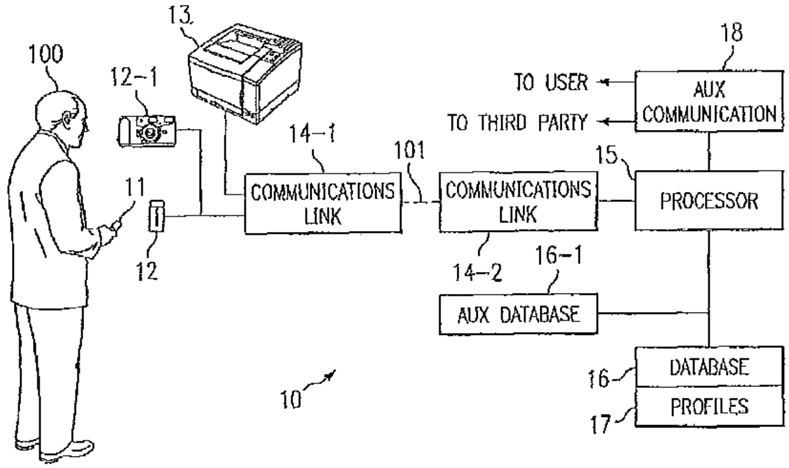
(Continued)

Primary Examiner — Thien M Le
(74) *Attorney, Agent, or Firm* — Snell & Wilmer L.L.P.

(57) **ABSTRACT**

A credit facility for controlling financial transactions is arranged with the ability of users to establish self-imposed limits on a category by category basis. The processing system provides messages and other information to the user, both on-demand and at the point of sale, based upon the category of the transaction and the limit set for that category. In one embodiment, both the user and, if desired, third parties, can obtain or be notified, of account balances on a category by category basis. Also, the main user can assign category limits, or prohibitions, on sub-users of the same account. In one embodiment, information pertaining to a specific transaction is communicated to a third party.

24 Claims, 7 Drawing Sheets



U.S. PATENT DOCUMENTS

5,790,668	A	8/1998	Tomko	
5,845,260	A	12/1998	Nakano et al.	
5,857,079	A	1/1999	Claus et al.	
5,870,723	A	2/1999	Pare, Jr. et al.	
5,914,472	A	6/1999	Foladare et al.	
5,953,710	A	9/1999	Fleming	
5,991,750	A	11/1999	Watson	
5,999,596	A	12/1999	Walker et al.	
6,006,205	A	12/1999	Loeb et al.	
6,026,370	A	2/2000	Jermyn	
6,045,039	A	4/2000	Stinson et al.	
6,070,141	A	5/2000	Houvener et al.	
6,173,269	B1	1/2001	Solokl et al.	
6,213,395	B1	4/2001	Dejaeger et al.	
6,224,109	B1	5/2001	Yang	
6,243,689	B1	6/2001	Norton	
6,308,887	B1	10/2001	Korman et al.	
6,325,285	B1	12/2001	Baratelli	
6,349,290	B1	2/2002	Horowitz et al.	
6,353,811	B1	3/2002	Weissman	
6,726,094	B1	4/2004	Rantze et al.	
6,728,397	B2	4/2004	McNeal	
6,796,497	B2	9/2004	Benkert et al.	
7,024,563	B2	4/2006	Shimosato et al.	
7,039,221	B1	5/2006	Tumey et al.	
7,152,042	B1	12/2006	Arkes	
7,231,068	B2	6/2007	Tibor	
7,246,243	B2	7/2007	Uchida	
7,254,548	B1 *	8/2007	Tannenbaum	705/18
7,444,305	B2	10/2008	Cotten et al.	
7,540,411	B1 *	6/2009	Tannenbaum	235/380
7,571,139	B1	8/2009	Giordano et al.	
7,631,193	B1	12/2009	Hoffman	
7,676,435	B1	3/2010	Berstis	
2001/0000535	A1	4/2001	Lapsley et al.	
2001/0011680	A1	8/2001	Soltesz et al.	
2001/0034720	A1	10/2001	Armes	
2001/0053239	A1	12/2001	Takhar	
2002/0016740	A1	2/2002	Ogasawara	
2002/0062279	A1	5/2002	Behrenbrinker et al.	
2002/0073416	A1	6/2002	Ramsey	
2002/0191816	A1	12/2002	Maritzen et al.	
2002/0194124	A1	12/2002	Hobbs et al.	
2002/0194137	A1	12/2002	Park et al.	
2003/0061111	A1	3/2003	Dutta et al.	
2003/0078849	A1	4/2003	Snyder	
2003/0154163	A1	8/2003	Phillips	
2003/0163708	A1	8/2003	Tang	
2003/0195859	A1	10/2003	Lawrence	
2003/0220841	A1	11/2003	Maritzen	
2004/0030654	A1	2/2004	Walker et al.	
2004/0039694	A1	2/2004	Dunn	
2004/0088221	A1	5/2004	Katz	
2004/0138958	A1	7/2004	Watarai	
2009/0083156	A1	3/2009	Cotten et al.	
2009/0234766	A1	9/2009	Tannenbaum	

FOREIGN PATENT DOCUMENTS

WO	WO01/73575	10/2001

OTHER PUBLICATIONS

"Manager", Retrieved from <http://www.credoreference.com/entry/chambdict/manage>, Chambers 21st Century Dictionary. London Chambers Harrap,(2001),2 pages.

"Advisory Action", U.S. Appl. No. 11/567,032, (Jul. 7, 2009),3 pages.

"U.S. Appl. No. 10/155,332", filed May 23, 2002,31 pages.

"U.S. Appl. No. 60/294,107", filed May 29, 2001, 11 pages.

"U.S. Appl. No. 60/458,096", filed Mar. 27, 2003, 13 pages.

"Restriction Requirement", U.S. Appl. No. 11/567,069, (Jun. 24, 2010), 6 pages.

"Non Final Office Action", U.S. Appl. No. 11/767,246, (Jun. 28, 2010), 24 pages.

"Notice of Allowance", U.S. Appl. No. 11/567,032, (Aug. 24, 2010), 8 pages.

"Non Final Office Action", U.S. Appl. No. 11/567,069, (Aug. 31, 2010), 9 pages.

Flaherty, Richard M., et al., "A New Twist on Credit for College Students", *Card News*, vol. 15, No. 16, (Aug. 9, 2000),3 pages.

"Final Office Action", U.S. Appl. No. 11/767,246, (Feb. 17, 2009),311 pages.

""Fraud"", *Chambers 21st Century Dictionary*. London: Chambers Harrap, Credo Reference, <http://www.credoreference.com/entry/2691119>.,(Feb. 4, 2009), 1 page.

""Secure"", *Collins English Dictionary*. London: Collins, 2000, Credo Reference <http://www.credoreference.com/entry/2691119>,(Feb. 4, 2009), 1 page.

"The Bank Credit Card Business", American Bankers Association, (1996),246 pages.

"Final Office Action", U.S. Appl. No. 11/567,032, (Apr. 2, 2009),20 pages.

"Non-Final Office Action", U.S. Appl. No. 11/567,032, (Nov. 24, 2009),16 pages.

"Final Office Action", U.S. Appl. No. 11/767,246, (Jan. 26, 2010),16 pages.

"Account", *Chambers 21st Century Dictionary*. London: Chambers Harrap, 2001, Retrieved from: <http://www.xreferplus.com/entry/chambdict/account> on Jan. 15, 2010,(2001), 2 pages.

"Final Office Action", U.S. Appl. No. 11/767,246, (Oct. 28, 2010), 23 pages.

USPTO; Office Action Restriction dated Oct. 27, 2005 in U.S. Appl. No. 10/192,426.

USPTO; Office Action dated Jan. 30, 2006 in U.S. Appl. No. 10/192,426.

USPTO; Office Action Restriction dated May 9, 2006 in U.S. Appl. No. 10/192,426.

USPTO; Final Office Action dated Oct. 23, 2006 in U.S. Appl. No. 10/192,426.

USPTO; Office Action dated Mar. 2, 2007 in U.S. Appl. No. 10/192,426.

USPTO; Notice of Allowance dated Jun. 18, 2007 in U.S. Appl. No. 10/192,426.

USPTO; Final Office Action dated May 2, 2011 in U.S. Appl. No. 11/567,069.

USPTO; Office Action dated Sep. 8, 2008 in U.S. Appl. No. 11/567,032.

USPTO; Office Action dated Apr. 8, 2008 in U.S. Appl. No. 11/567,044.

USPTO; Final Office Action dated Oct. 16, 2008 in U.S. Appl. No. 11/567,044.

USPTO; Notice of Allowance dated Jan. 28, 2009 in U.S. Appl. No. 11/567,044.

USPTO; Office Action dated Oct. 22, 2008 in U.S. Appl. No. 11/767,246.

* cited by examiner

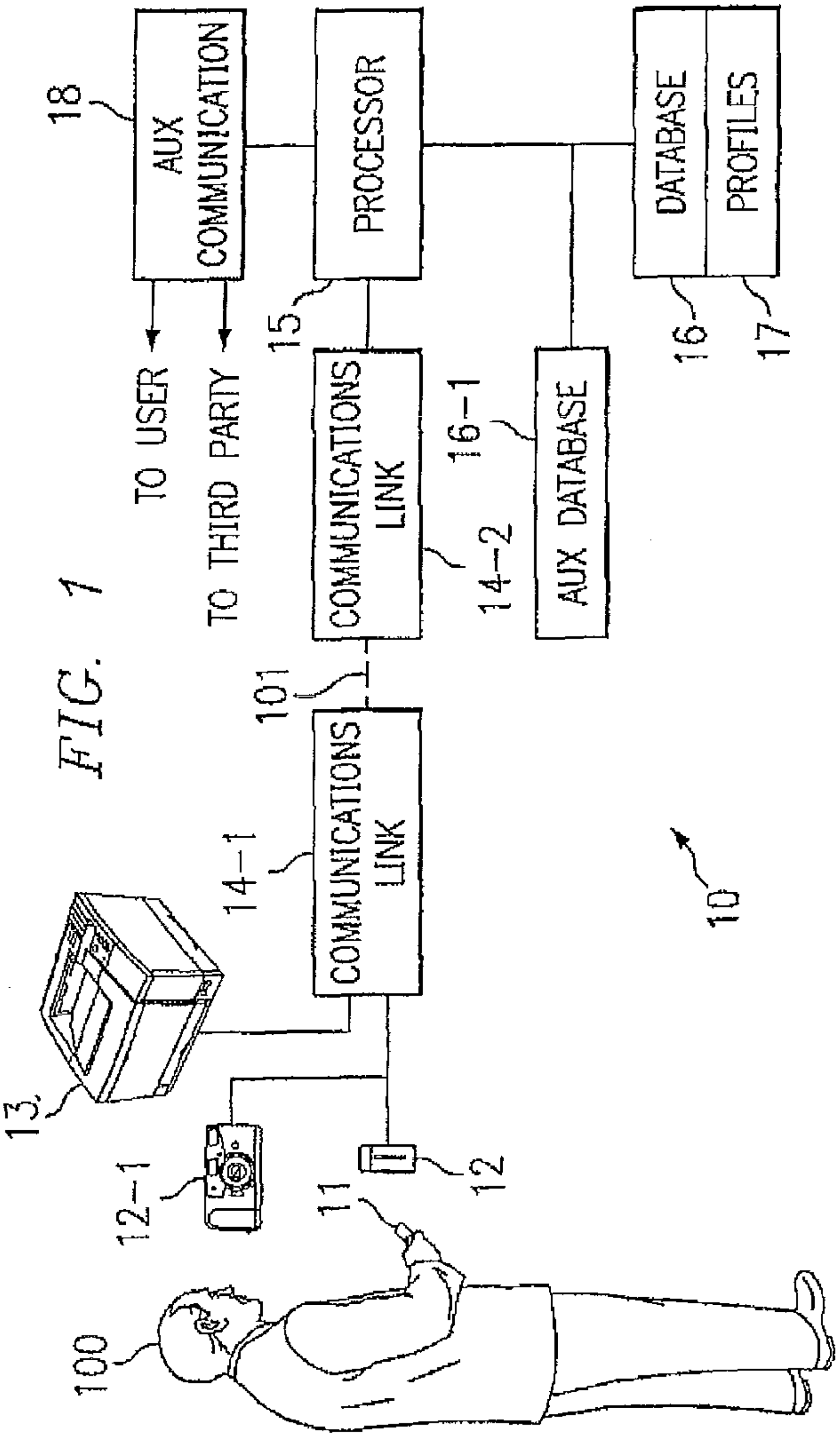

18
AUX COMMUNICATION
PROCESSOR
DATABASE
PROFILES
TO USER
TO THIRD PARTY
15
16
17
COMMUNICATIONS LINK
16–1
AUX DATABASE
14–2
101
COMMUNICATIONS LINK
14–1
13
12–1
11
12
100
10

FIG. 1

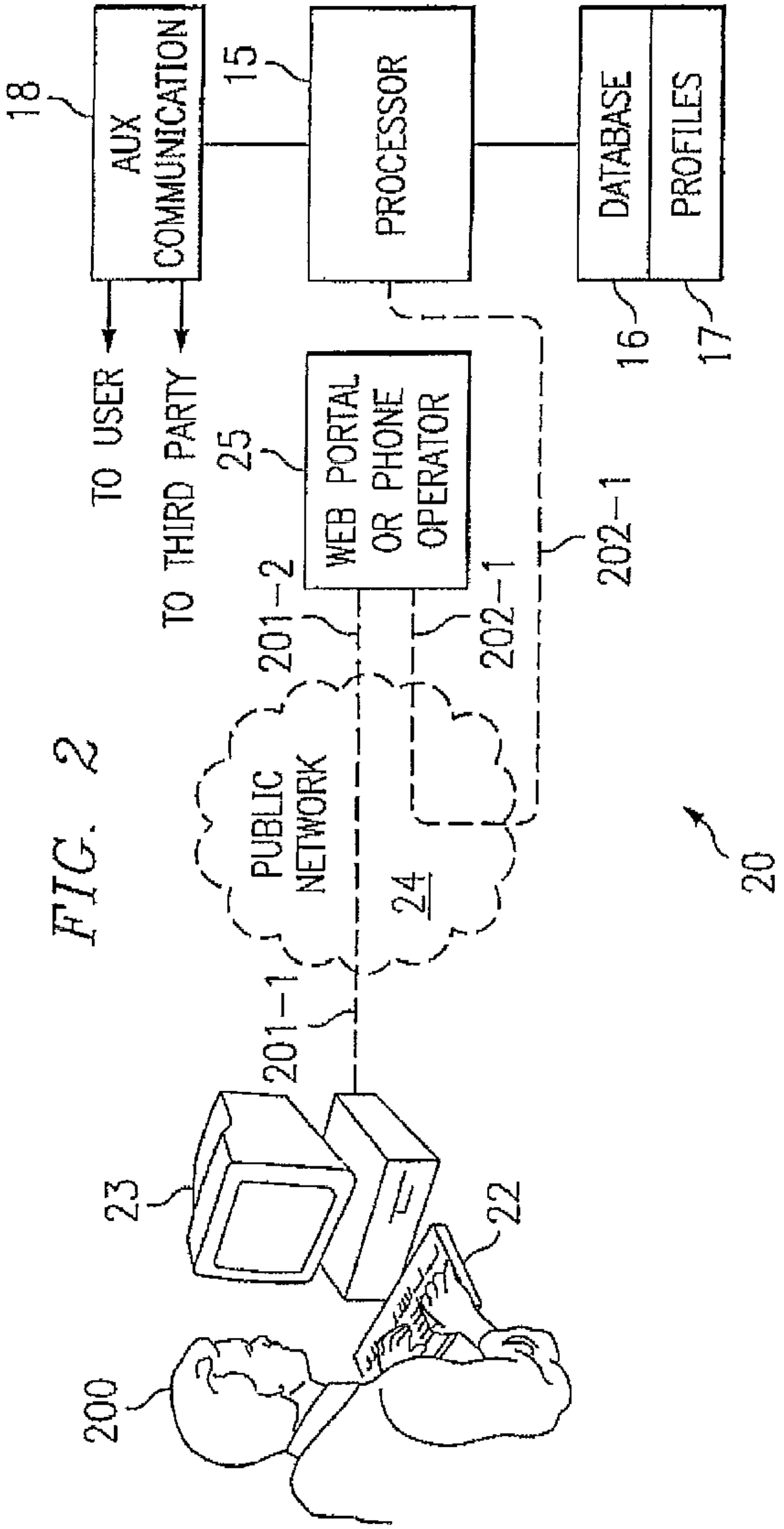


FIG. 2
18
AUX COMMUNICATION
15
PROCESSOR
DATABASE
PROFILES
16
17
TO USER
TO THIRD PARTY
25
WEB PORTAL OR PHONE OPERATOR
201-2
202-1
202-1
PUBLIC NETWORK
24
201-1
20
23
22
200

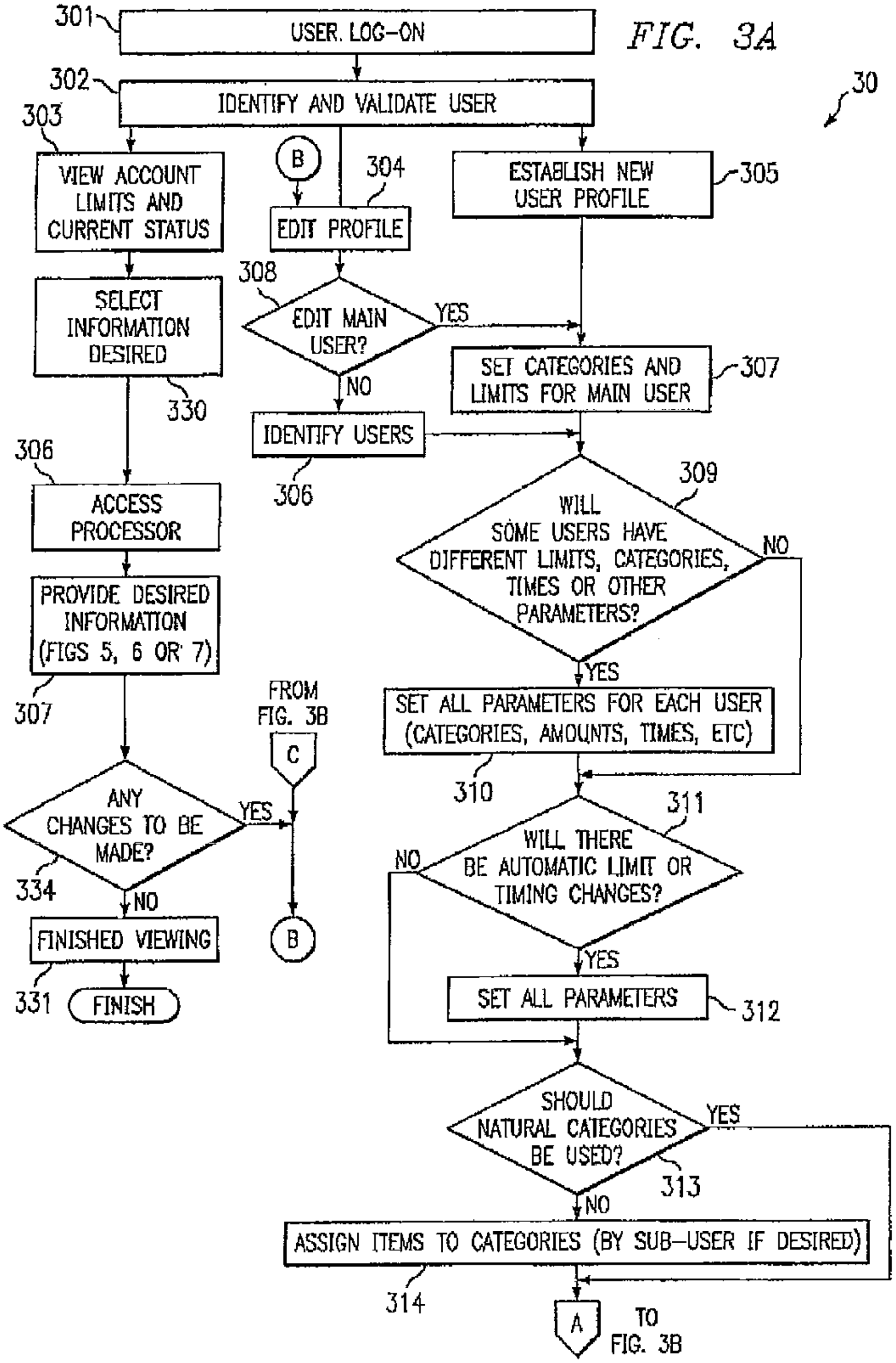
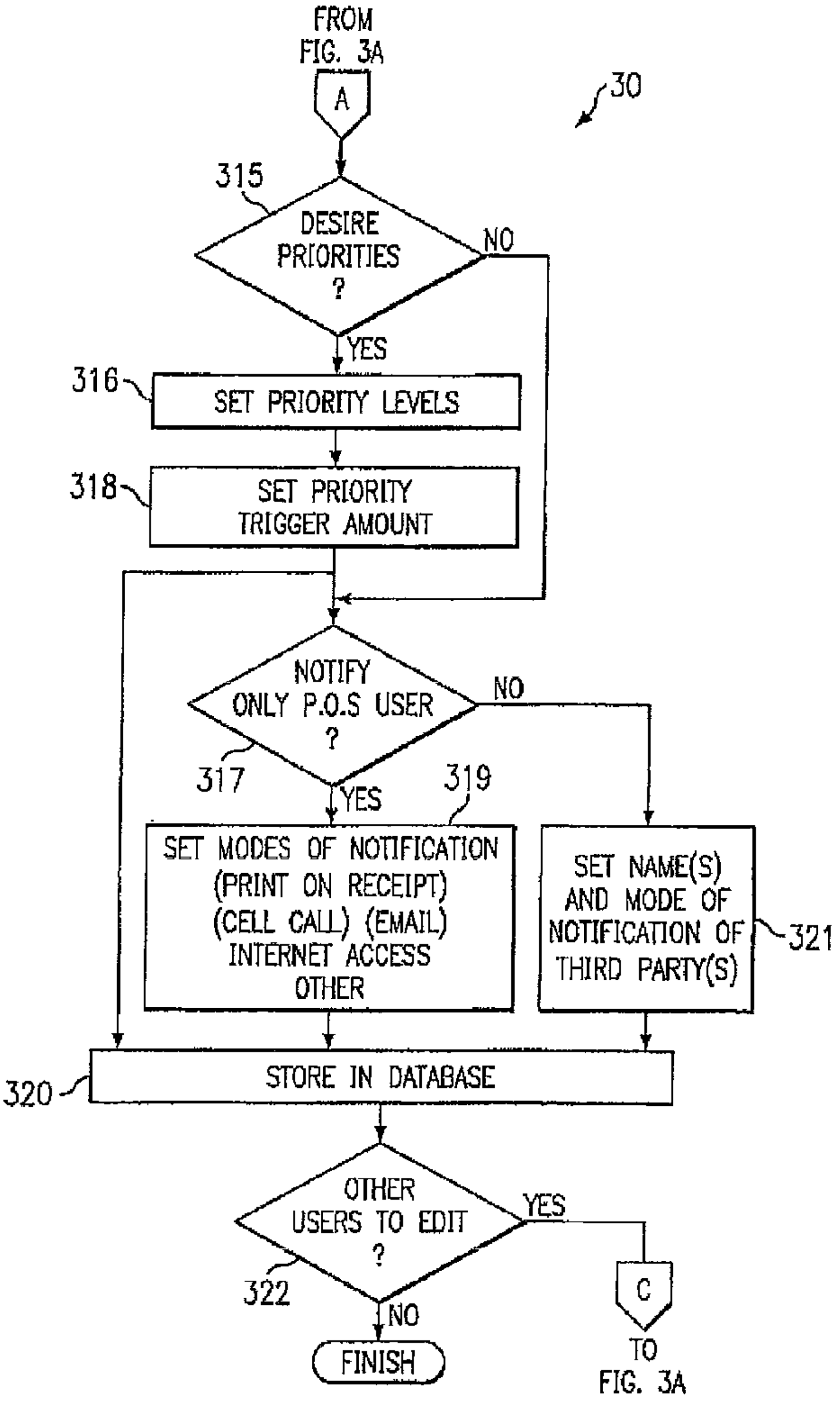


FIG. 3A
30
301
USER LOG-ON
302
IDENTIFY AND VALIDATE USER
303
VIEW ACCOUNT LIMITS AND CURRENT STATUS
B
304
EDIT PROFILE
ESTABLISH NEW USER PROFILE
305
SELECT INFORMATION DESIRED
308
EDIT MAIN USER?
YES
NO
SET CATEGORIES AND LIMITS FOR MAIN USER
307
330
IDENTIFY USERS
306
306
ACCESS PROCESSOR
309
WILL SOME USERS HAVE DIFFERENT LIMITS, CATEGORIES, TIMES OR OTHER PARAMETERS?
NO
YES
PROVIDE DESIRED INFORMATION (FIGS 5, 6 OR 7)
307
FROM FIG. 3B
C
SET ALL PARAMETERS FOR EACH USER (CATEGORIES, AMOUNTS, TIMES, ETC)
310
ANY CHANGES TO BE MADE?
YES
334
NO
311
WILL THERE BE AUTOMATIC LIMIT OR TIMING CHANGES?
NO
YES
FINISHED VIEWING
B
331
FINISH
SET ALL PARAMETERS
312
SHOULD NATURAL CATEGORIES BE USED?
YES
313
NO
ASSIGN ITEMS TO CATEGORIES (BY SUB-USER IF DESIRED)
314
A
TO FIG. 3B

FIG. 3B


FROM
FIG. 3A
A
30
315
DESIRE PRIORITIES ?
NO
YES
316
SET PRIORITY LEVELS
318
SET PRIORITY TRIGGER AMOUNT
NOTIFY ONLY P.O.S USER ?
NO
317
YES
319
SET MODES OF NOTIFICATION (PRINT ON RECEIPT) (CELL CALL) (EMAIL) INTERNET ACCESS OTHER
SET NAME(S) AND MODE OF NOTIFICATION OF THIRD PARTY(S)
321
320
STORE IN DATABASE
OTHER USERS TO EDIT ?
YES
322
NO
FINISH
C
TO
FIG. 3A

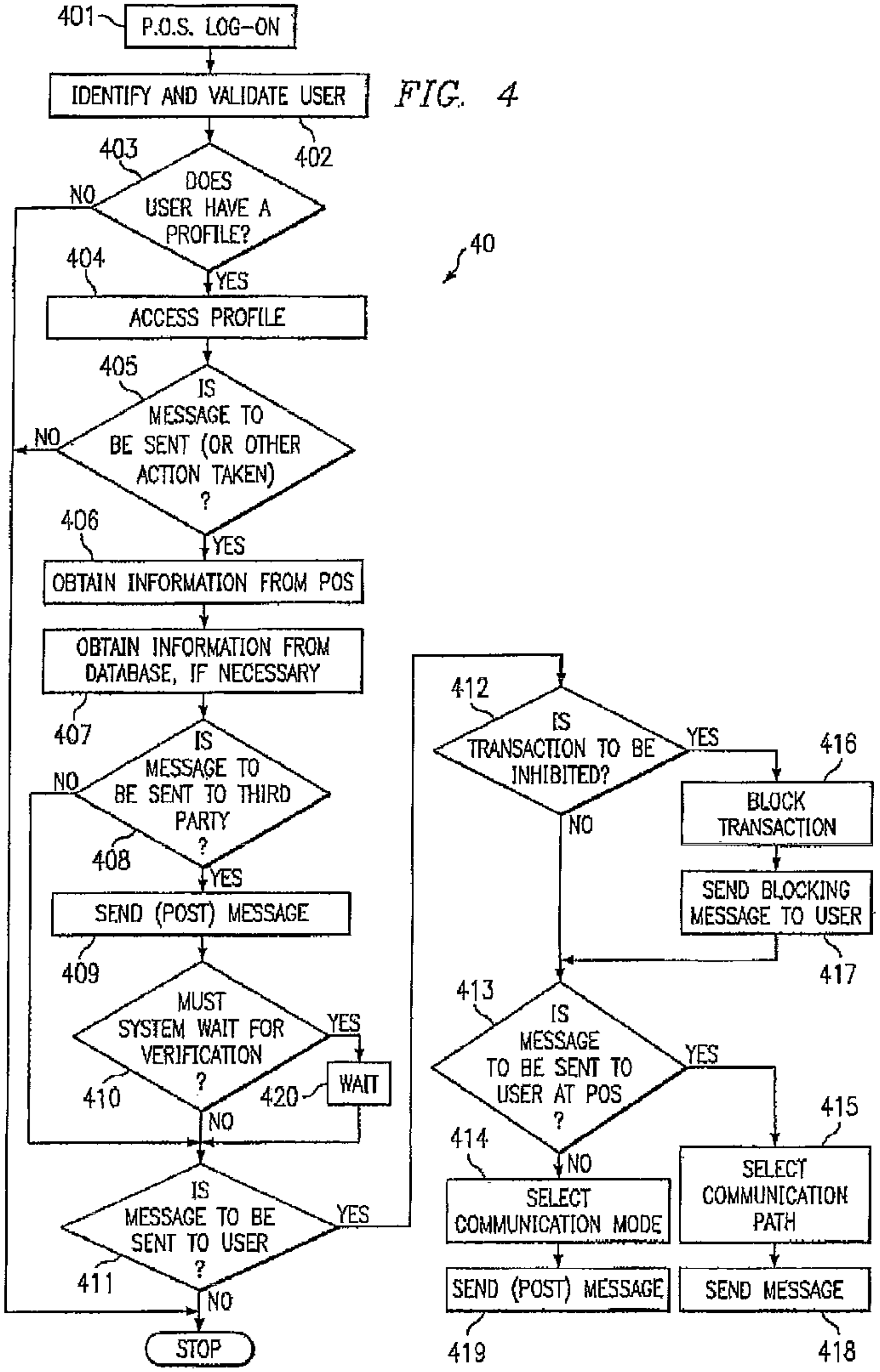


FIG. 4

401
P.O.S. LOG-ON
IDENTIFY AND VALIDATE USER
402
403
DOES USER HAVE A PROFILE?
NO
YES
40
404
ACCESS PROFILE
405
IS MESSAGE TO BE SENT (OR OTHER ACTION TAKEN) ?
NO
YES
406
OBTAIN INFORMATION FROM POS
OBTAIN INFORMATION FROM DATABASE, IF NECESSARY
407
IS MESSAGE TO BE SENT TO THIRD PARTY ?
NO
YES
408
SEND (POST) MESSAGE
409
MUST SYSTEM WAIT FOR VERIFICATION ?
YES
WAIT
420
410
NO
IS MESSAGE TO BE SENT TO USER ?
YES
NO
411
STOP
412
IS TRANSACTION TO BE INHIBITED?
YES
NO
416
BLOCK TRANSACTION
SEND BLOCKING MESSAGE TO USER
417
413
IS MESSAGE TO BE SENT TO USER AT POS ?
YES
NO
414
415
SELECT COMMUNICATION MODE
SELECT COMMUNICATION PATH
SEND (POST) MESSAGE
SEND MESSAGE
419
418

50

FIG. 5

CATEGORY	CODE	AMOUNT	PRIORITY	ACCOUNTING PERIOD	ADJUSTMENT AMOUNT	ADJUST	USER (PIN)
FOOD	01	$200	1	WEEKLY	$100	JULY-AUG	ALL
SNACKS	02	$50	2	MONTH	$50	JULY-AUG	ALL
CLOTHING	03	$150	2	MONTH	$500	AUG	ALL
RESTAURANTS	04	$200	3	MONTH	$300	JULY	A
BOAT	05	$1000	3	SEMI-ANNUAL	–	–	B
TRAVEL	06	$4000	2	SEMI-ANNUAL	–	–	A, B
GIFTS	09	$50	2	MONTH	$2000	DEC	A, B
ENTERTAIN	10	$400	3	MONTH	–	–	A
OVERALL	00	$2000	–	ANYTIME	$2000	DEC	
ALCOHOL	11		BLOCKED				NONE

60

FIG. 6

STORE	ITEM	NATURAL CATEGORY	PROFILE CATEGORY
SUPERMARKET	MEAT	FOOD	FOOD
SUPERMARKET	POTATOES	FOOD	FOOD
SUPERMARKET	VEGETABLE	FOOD	FOOD
SUPERMARKET	COOKIES	FOOD	SNACKS
SUPERMARKET	ICE CREAM	FOOD	SNACKS
SPORT STORE	FISHING GEAR	SPORT	BOAT
DEPARTMENT STORE	SHIRTS	CLOTHING	CLOTHING
DEPARTMENT STORE	SHOES	CLOTHING	CLOTHING
SPORT STORE	SHOES	CLOTHING	BOAT
CABLE COMPANY	CABLE TV	ENTERTAIN	HOME

70

FIG. 7

ITEM	STORE	DESCRIPTION	AMOUNT	CATEGORY	PROFILE BUDGET	ACTUAL PERIOD	ACTUAL BUDGET	YEAR TO DATE	CHANGE
X1035	VIDEO	MOVIE RENTALS	$20	ENTERTAIN	$100	MONTH	$145	OVER	HOME
3801	THEATER	MOVIE	$30	ENTERTAIN	$100	MONTH	$145	OVER	–
–	CABLE	CABLE	$45	ENTERTAIN	$100	MONTH	$145	OVER	HOME
1202	BOOK	NOVEL	$10	ENTERTAIN	$100	MONTH	$145	OVER	
1209	BOOK	TRAVEL BOOK	$20	ENTERTAIN	$100	MONTH	$145	OVER	TRAVEL
–	BIG T	MEN'S SHOES	$80	CLOTHING	$100	MONTH	$230	UNDER	BOAT
–	BIG T	CHILDREN'S SHIRTS	$50	CLOTHING	$100	MONTH	$230	UNDER	–
3351	DEPARTMENT STORE	MEN'S SHOES	$100	CLOTHING	$100	MONTH	$230	UNDER	–

ADMINISTRATION OF FINANCIAL ACCOUNTS

RELATED APPLICATIONS

This application claims priority to U.S. application Ser. No. 11/567,044 which, in turn, is a divisional of and claims priority to U.S. application Ser. No. 10/192,426, now U.S. Pat. No. 7,254,548. This application also claims priority to U.S. patent application Ser. Nos.: 11/567,032; 11/767,246; and 11/567,069, all of which claim priority to U.S. Pat. No. 7,254,548. The subject matter of U.S. Pat. No. 7,254,548, and application Ser. Nos. 11/567,044; 11/567,032; 11/767,246; and 11/567,069 is expressly incorporated by reference herein.

BACKGROUND

The popularity of credit cards, debit cards, and other facilities for financing transactions for the consuming public at the point of sale is now without question. It is easy, and all too prevalent, that along with such popularity and ease of use of most point of sale credit facilities, comes financial difficulty for many people.

It is difficult, even for the most disciplined person, to resist the temptation of purchasing a product spontaneously. This impulse buying is often encouraged by merchants and, when done well, is highly effective.

Today, most credit facilities, such as credit cards, have ultimate spending limits, such that when the limit is exceeded (or the most recent invoice not paid promptly) the consumer user is denied further access to credit. Usually, by this time, the consumer is in financial distress.

Many credit facilities today allow consumer users to obtain current balances, as well as recent purchase information, by telephone or Internet, or other on-line access. This historical data does not adequately address the problem, as it does not help the consumer in making purchasing decisions at the time a purchase decision is being contemplated. Also, many credit facilities give annual print-out summaries of purchases by category. While such reports are nice to have at tax season, or for next year's planning, they are a backward-looking view and do not serve to help the consumer on a day-to-day basis. People on fixed incomes, low incomes and people with debt "problems," should be on rigid budgets and may require current financial information in a more timely manner. People striving simply to "watch" their spending also require current information, if they are to make intelligent buying decisions.

Another problem exists today when some users have the use of a card issued to another person. For example, in an employer/employee situation often an employee is given use of a credit card for the purchase of goods or services which are business related. Unfortunately, such credit facilities are sometimes misused, or the balances go too high, and by the time the employer learns of the problem it may be too late to remedy the situation.

SUMMARY

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

Various embodiments are directed to a system and method which allows consumer users to establish self-imposed limits on the user's spending (borrowing) such that when the limit is reached the consuming user is notified. This notification can be before, during or after the point of sale transaction, and can be delivered, if desired, by the account clearing network and printed on the user's purchase receipt. The notification message can be delivered via a phone call, email or over an Internet connection to the user. The notification can be to one or more designated third parties, such as a parent, or card owner, or a debt counselor.

In at least one embodiment, the user will pre-establish self-imposed spending limits (guidelines) on a category by category basis, and each category can have, if desired, a different accounting period. For example, the food category can have a monthly (or weekly) limit, while the hobby category can have, for example, an annual or semi-annual limit. Since these limits are self-imposed, they do not impact the user's ability to complete any transaction, but rather they serve to provide the user meaningful information at a time when that information is most useful.

In another embodiment, the user may access his/her account, other than at the point of sale, to see (or hear) a running total of category balances, based on accounting periods, as well as comparisons against the user imposed pre-established category by category budget.

In another embodiment, the user can establish the limits, and can change the limits when desired, by telephone, email, Internet or the like. Also the limits need not be constant from accounting period to accounting period. Thus, if a person's ability to repay the charged (borrowed) amount fluctuates during the year, the user may pre-establish that the limits will automatically change during those periods. Also, the user might decide that if his/her total outstanding balance reaches a certain amount, certain budgeted categories then will be reduced until the total unpaid amount recedes below the "critical" level. In this regard different categories can be given different priorities.

For example, assume a user has a total line of credit of, say, $5,000. Also assume that the user has established that his/her food budget is to be $200 per week (with the highest priority set), and that the boat budget is $1,000 per year (with the lowest priority set). Also let us assume that the user has set a self-imposed arbitrary cap on his/her outstanding credit card balance of, $2,000, let us assume also that the current outstanding balance has exceeded the self-imposed $2000 limit, but has not reached the $5,000 card limit.

Now let us assume that the user desires to buy a new $100 fishing rod for his boat and this will be the first "boat" purchase this year. The user can access his account in any number of ways, for example, by voice, or by Internet or at the point of sale. When the user accesses the account, since the self-imposed outstanding balance cap of $2,000 has been exceeded, the user will be informed that the available budget for the fishing rod is zero, even though the available budget amount is $1,000 and even though the line of credit still allows for $3000 worth of spending. Note, that had the user inquired about a food category he/she would have been told the actual amount available (or the actual amount used, if desired) in the "food" category.

In a still further embodiment, the user may establish sub-users on his/her account and may authorize each user to use the account only with respect to certain categories, or category amounts, or only up to a certain credit limit, or only for a certain period of time, or a combination of the above.

The foregoing has outlined rather broadly the features and technical advantages of the various embodiments in order that the detailed description of the embodiments that follows may be better understood. Additional features and advantages will be described hereinafter which form the subject of the claimed subject matter. It should be appreciated by those skilled in the art that the conception and specific embodiments disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the described embodiments. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the claimed subject matter as set forth in the appended claims. It is to be expressly understood that each of the figures is provided for the purpose of illustration and description only and is not intended as a definition of the limits of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the claimed embodiments, reference is now made to the following descriptions taken in conjunction with the accompanying drawing, in which:

FIG. 1 shows a block diagram of one embodiment where the credit-card user is making a purchase at a point of sale located at a merchant's premises;

FIG. 2 shows a block diagram of another embodiment where the credit card user is making a purchase, editing a profile or obtaining account information via an on-line Internet (or telephone) connection;

FIGS. 3A and 3B show one embodiment of an operation where the user obtains information from and/or edits his/her profile;

FIG. 4 shows one embodiment where the processing system, in response to a request, provides a message and/or blocks the transaction dependant, in part, upon the information contained in the user's profile;

FIGS. 5 and 6 show embodiments of profile data bases on a category by category basis; and

FIG. 7 shows one embodiment of a user account organized by category.

DETAILED DESCRIPTION

Turning now to FIG. 1, there is shown System 10, which is one embodiment showing user 100 with credit card 11, getting ready to insert the card into card reader 12 to complete a sales transaction at a point of sale. The information from card reader 12 is communicated via communications links 14.1 and 14.2 and network 101 to central processor 15. Processor 15, in conjunction with database 16 and profiles 17, then categorizes the various purchases being made and stores those purchase amounts and categories in database 16, according to profiles of user 17, as stored, for example, in profile data base 17.

As will be discussed, these profiles can include not only the budget amounts for each category, but what types of items would fit into the different categories. Based upon the profiles, processor 15 then can communicate in one or more of several ways, such as, for example, back over communications links 14-1, 14-1 to user 100 or over alternate communication paths via auxiliary communication 18. This communication can be, for example, via printer 13, or it can be via auxiliary communication path 18. Auxiliary communication 18 can be, for example, to the user via cell phone, pager, or other device. At the same time, if desired, third parties, such as parents, employers, debt counselors and others, could also be notified. This communication can, if desired, occur for all purchases, or for certain of the purchases by category or by amount.

The system can be designed, if desired, such that if the amounts in a category (or if the total outstanding balance at that time) were to exceed a certain amount, user 100, or a third party as identified in the user's profile, would be required to give specific approval for a particular purchase. This system could be extended so that third parties (such as parents) can allow a child to use a credit card, but certain purchases over a certain amount, or all purchases, or purchases in certain categories, will require approval from the parent (or other third party), who would not actually be present at the point of sale.

For example, a parent could allow a child to have a credit card for the purpose of buying clothes. The child then selects his or her purchases at a location and runs card 11 through the card reader at the point of sale. The system, via profile 17, database 16 and processor 15, then recognizes that this is a card which is a sub-account card of a main account, or an account that is otherwise special to this person. Processor 15 then enables a communication to the third person identified by profile 17 via auxiliary communication 18. This communication could be, for example, cellular, landline, Internet, pager, PDA, or the like. The purchase can only be completed, if the third person responds in a positive manner (perhaps by pushing a button or speaking an acceptance word as set out in the user's profile). Processor 15, perhaps working in conjunction with other network processors, controls the acceptance back to the point of sale.

In some situations, it could be appropriate for the item that is being purchased to have a picture, available either in an auxiliary database 16-1, or transmitted from the point of sale at the time of purchase, transmitted to a third person, either for approval or simply for information purposes. This would be helpful, for example, when a husband is buying a suit and wants his wife to see the suit before the purchase is consummated. A picture of the suit could be captured by camera 12-1, communicated over the communication link to processor 15, and then through auxiliary communication 18 to a designated third party at a cell phone, computer, pager, FDA, or the like.

In some situations, the purchaser may desire additional information, such as warranties, specifications, pictures, assembly instructions, to be sent to a specific location (such as the point of sale, or to his/her home), or the purchaser may wish to register his/her purchase with the seller, or even apply for a rebate, all at the time or purchase. Processor 15, working in conjunction with database 16 and profiles 17 then could send the purchaser's address and other information to the seller. The seller's information obtained from transmitted POS information, or from data contained at the central location, such as from auxiliary database 16-1, would be combined with the user's (purchaser's) information as obtained from database 16, and sent to the seller. Since the user specific database contains information pertaining to the user's prior purchases it could be used, for example to aid the purchaser in making new purchases, perhaps by providing compatibility information to the user, either at the POS or on demand. This compatibility information could be within system 10, but would likely reside with each specific seller and could be supplied to the user at the POS (or on demand) in response to the above-discussed purchase registration.

Note that auxiliary database 16-1 can hold any type of information that is desired to be communicated to either user 100 or to third parties. This information could be sound, video, or any type of information, and can be stored in compressed format in the well-known manner. Also the information sent to a third party could be, for example, pictures, video, color, audio or any combination thereof. In addition, the information could be partially located in the database, such as database 16-1 and available based upon some information, perhaps a bar code or other information sent from card reader 12 or from camera 12-1.

In addition, the system could use camera 12-1 to take a live picture of user 100 at the point of sale and to then match that picture against a known picture or other information. This could then be sent to a third party for verification based upon a profile in database 17. Thus, when a main user of a credit card allows other sub-users, which could be employees, children, relatives, temporary workers, to use the sub-account card, each purchase using the sub-account card could trigger, if desired, the taking of a picture of the then user at the POS. This picture, or other information (such as a password) could be transmitted, under control of profile 17, database 16 and processor 15 to the main user, as discussed above, such that the transaction would not be completed until the main user signified acceptance.

This system, for example, could be used to keep an account "open" for the real user for a period of time when a card is reported lost or stolen. In such an event, the profile would be used to provide the system with a special verification procedure unique to the user. This verification could be for example, a password necessary at each purchase, or a biometric sent from the POS for comparison during each transaction.

System 10 could operate such that the main user, as will be discussed, can at any time change his/her profile, thereby adding or changing passwords, and assigning passwords or other control information to the profile. These passwords could be for the main account, or for any sub-account. When the credit card is presented at a POS, system 10 would check the user's profile to see if any such passwords, third party approvals, etc, are required. If so, the salesperson at the point of sale could then follow directions sent to that person via network 101 so as to obtain the proper identification of the user. This would give an added measure of security to credit card users. For example, the profile of a user might specify that call-in purchases (ones where the card is not physically present at the POS location) will need to be verified by a specified password, or verified by a communication placed by the salesperson (or by system 10) to a third person. The user's own created profile will allow for flexibility in this regard.

Note that the profile of the user, including database information if desired, could be stored on the user's card along with, if desired, at least some of the processing. In such a scenario, information from the profile would be sent to a central processing network to provide the services for the user as discussed above. A so called "smart card" would be one method of accomplishing this objective.

Turning now to FIG. 2, there is shown System 20 in which user 200 is utilizing keyboard 22 and computer 23 to access his or her account via communication links 201-1 and 210-2 and public network 24 to web portal or phone operator 25. Portal 25 then accesses processor 15 via communication link 202-1. Such accessing of the system by user 200 could be for the purpose of obtaining account information at any time on a category by category basis, or for establishing (as will be discussed) various account categories, balances and sub-users, or user 200 could be using computer 23 (which could be a telephone, pager, PDA, or the like) as a POS device. Note that connection 201-1, as well as the other connections shown, could also be by pager network, cellular network or any other type of network, including for example, wireless, wire line or the cable satellite network typically utilized for broadcast signals into the home for entertainment purposes. Once connected to processor 15, the system operates as discussed above with respect to FIG. 1. In the situation where at least a portion of the processing is on the user's smart card, then the user would insert his/her card at a reader (not shown) associated with computer 23. Of course, if the smart card included wireless technology, such a reader would be unnecessary, both in FIG. 2 as well as in FIG. 1.

FIG. 3A shows system 30 which is one embodiment of a system utilized to enable system 10 (FIG. 1), or system 20 (FIG. 2) where a user can establish various categories and credit limits and/or view the existing account at any time. In process 301 the user logs onto the system as is well known. In process 302 the user is identified and is validated by the system. At this point the user is given several choices, three of which are shown in FIG. 3A. One such option, as shown in process 303, allows the user to view the account limits and current status. The user in process 304 could edit the profile and in process 305 the user may establish new profiles.

Assuming the user wanted to view the account limits, then the user in process 330 would select the desired information. The system in process 306 would access the processor and other databases and profiles to provide the desired information, via process 307, which could be in the form of FIG. 5, 6 or 7, or other profile information. If the user desired to just view the information, process 334, then when the user was finished, as shown by process 331, the connection would be terminated in a well known manner.

If changes were to be made, as controlled by process 334, then the user would be directed to edit profile process 304, and the user could either edit the main user or subusers. Assuming the main user is to be edited, the user is directed to the same path as would be utilized if there was to be established a new profile via process 305, such that the user, under control of process 307 would set the categories and limits for the main user.

Going back to process 308, had the main user decided to edit some profile other than the main user's profile, then the users would be identified via process 306 and the paths then would be concurrent for both the sub-users' and main user, such that process 309 would inquire as to whether some users would have different limits, categories, times or parameters.

If the answer was yes, then those parameters would be set for each user as to which category, amount, time or any other parameter desired for individual sub-users and the main user. If everybody were to have the same limits, then process 309 would skip to process 311 and the question would be answered as to whether there are automatic limits with timing changes to be applied. If there were, those parameters would be set via process 312. Process 312 would also control any other parameter that needed to be set, such as, by way of example, the user's home address, phone number, email address, auxiliary addresses (both physical and electronic), cell phone numbers, pagers, PDA addresses, third party notifications, together with their respective contact information, passcodes, special limits.

After the user is finished entering all of the desired parameters, the question would be asked as to whether the normal categories of purchase goods were to be used. By this it is meant that some categories would be preset by the system itself, such that clothes being purchased would always go under the clothing category. However, if desired, a user could decide that clothes from certain stores, or certain types of clothing, such as sporting clothes, would go under a sporting category. The user could decide, for example, such that certain foods would go under a discretionary category other than food. This can be seen in FIG. 6 where the natural category for, say ice cream, would be food, but a user could switch the natural category to a profile category of snack, if desired. Likewise, fishing gear would have a normal category of sporting goods, whereas this user would have a profile category of boating. This would allow a user to more finely tailor his or her profile to be more accommodating of the user's needs. It would allow a fine tuning of budgeting and expenses on an 'as you go' basis.

In process **314**, the user can assign items to categories and can do so by sub-user if desired, so that certain sub-users can have access to all categories, or some categories, and also what items are included in those subcategories. For example, a parent may allow a child a credit card for the purchase of food, and restrict the child from buying alcohol or cigarettes, if so desired. Or, the parent could allow the child to have a credit card for the purchase of gasoline for the family car, but other products sold at the service station would fall into a different category, either naturally or as a selection under the categories selected under process **314**, such that only certain products such as gasoline could be purchased by certain users of the credit card.

Continuing on FIG. 3B, if the user desired to set priorities for different categories, process **315**, such that as discussed above, based upon the priority level set in process **316**, and the trigger amounts in **318**, the user would be notified of different category levels such that the user is better able to maintain a strict budget when necessary. Since these limits are all self-imposed the user can determine, on a category by category basis, the difficulty and manner for overriding any "inhibiting" message.

In process **317** it is determined whether only the point of sale user is to be notified, and if so, how that notification is to be made via process **319**. Notification can be printed on the receipt, or the notification can be by cellular phone call, email or other notification and can be contemporaneously with the transaction or thereafter. If third parties are to be notified, then the names of the third parties and mode of notification can be set via process **321**, all of which would be stored in database **16** and profile **17** (FIG. **1**) via process **320**.

Before exiting the system, the user may wish to edit the profiles, perhaps to add other people or other categories, limits or the like. If so the system recycles back to process **304**, FIG. 3A. If not, the user is finished with the profile.

Turning now to FIG. **4**, there is shown system **40** which illustrates one embodiment of the point of sale transaction where the user is in the process of buying a product using a credit facility. The user typically would have a card swiped through a reader, as discussed in FIG. **1**. This operation is shown by processes **401** and **402**. System **40** would then determine via process **403** whether the user has a profile. If not, the system would proceed as normal, in the well known manner.

If the user has a profile, then the profile is accessed via process **404** and the profile then begins to control the transaction at the point of sale. If there is not a message is to be sent to the user, or to a third party, and if no other special action is to be taken, then the system would proceed normally. If special POS actions are required, then the system would obtain any appropriate information from the point of sale via process **406**. This information can be information from the specific transaction, such as items purchased, categories, amounts of each item. Or it could be information pertaining to the user, such as for example, a picture of the user, iris scan, fingerprint, or other biometric. In this case the picture (or other information) of the user would become an item to be stored and perhaps sent to third parties for verification of the transaction, or simply for record purposes. The information from the POS could be a user response, such as, for example, the mileage on a car. This information could then be used by the system to calculate the user's gas mileage (miles per gallon) based on "Gas" category purchases and user supplied information.

If necessary, process **407** would utilize POS information, such as bar codes or other category information, to then obtain other data from a data base. For example, based upon a bar code obtained from the POS, information could be sent back to the user at the POS or could be forwarded to one or more third parties, perhaps for verification, or for registration, or the like. Pictures of the purchased items could be obtained, along with specifications, warranty information, last minute updated information (such as usually contained in a Read Me file) and sent to the customer at the point of sale, if desired. If a message is to be sent to a third party via process **408**, then this message is either sent or posted via process **409**. Another example, would be for the system, based on profiled information, to send third party and address information back to the user, perhaps so that the user can send a purchase to the third party.

If the system must wait for verification from a third party, as contained in process **410**, then process **420** controls this waiting period and the POS transaction stops until the desired information is returned. This information could be approval or other information from third parties, or it could be service contract information, specification information, or other types of information desired by a customer.

Then it is determined if a message is to be sent to the user. This message could be the overall account balance, or a category account balance, or if desired a summary of category balances. This information can be delivered before the completion of the transaction, or afterward, and it could be contained on a receipt generated at the POS or it could be a communication to a third party, all determined by the profile of the user.

Process **412** controls as to whether the transaction is to be inhibited in any manner. If it is, inhibiting (or blocking if desired) is controlled by processes **416** and **417**. If it is not to be inhibited, a determination must be made if a message is to be sent to the user at the point of sale, or other places as controlled by processes **413**, **414**, **415**, **418** and **419**. If the transaction is to be inhibited, this is controlled by processes **416** and **417**, all under pre-control of the user.

FIG. **5**, as discussed above, shows different categories, codes for categories, amounts that the user has decided upon, the priority of the category, the accounting period for the priority, and how much the category can be adjusted and when the adjustment would occur.

For example, in the food category, the amount is $200.00 per week, but during the months of July and August, this is adjusted by $100.00 to take into account the different food intake needs of the family during vacation periods. In this case, all users have access. Code **4**, which is restaurants, is a monthly account of $200.00 for eating out at restaurants. It is adjusted by $300.00 during the month of July, and the only user that can use it is the A user. The boat account is $1,000.00. It is a semi-annual amount and has a priority **3**, which if desired, means that if other categories are over at a particular time when the boat account is to be used this account will be inhibited (subject to being overridden by the user) until the overall account balance goes below a certain amount.

As shown in the example, only the B user can buy purchases in the boat account. For this user account alcohol is a code inhibited for all users. Thus this account, regardless of who the user is, cannot buy alcohol because of the self-imposed prohibition. Of course, such prohibitions could apply to any category, such as tobacco, movies, etc., as established by the user of the account. These prohibitions can be on a category by category basis and can be more finely granulated so that sub-user accounts can each have different permission levels if desired.

FIG. 6 shows different natural categories that have been changed to the profile categories, depending upon the specific needs of this user. Thus, when the system processes purchases in certain natural categories, these categories are "translated" into the categories that the user desires. Thus, as discussed above, instead of ice cream being classified as a food, for this user, ice cream would be accounted of in the category called snacks.

FIG. 7 shows a sample printout of information that is available to the user on demand of the user. This information can be periodically delivered to the user, or the user can obtain the information on-line via, for example, the Internet. The available information shows usage by category according to the specific profile of the user. This then allows the user to plan purchases and to know at any time where the user is with respect to the user's own budget.

Of course, FIG. 7 can be arranged in any way and the information can be provided in different formats, and it even could be arranged as the user would like it to be, based upon user designed formats.

It should be noted that while the example discussed above is an example using a credit card, the term credit facilitation system can be a credit card, a debit card, a smart card or even a card issued by a specific store, chain or organization for the purpose of providing discounts and/or identity for particular users.

Although the described embodiments and their advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the claimed subject matter as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same results as the corresponding embodiments described herein may be utilized according to the present teachings. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

What is claimed is:

1. A system comprising:

means for storing a profile keyed to a user identity and containing one or more user-selected categories to track transactions associated with said user identity, wherein individual user-selected categories include a user pre-set limit; and

means for presenting transaction summary data for at least one of the one or more user-selected categories, said transaction summary data containing said at least one user-selected category's user pre-set limit.

2. The system of claim 1, wherein the individual user-selected categories further include one or more purchasable items.

3. The system of claim 2 further comprising means for assigning individual purchasable items to one or both of: a natural category or a user-specified category.

4. The system of claim 1, wherein said at least one user-selected category is associated with one or more user-selected sub-user identities, and wherein said transaction summary data includes one or more sub-user transactions associated with at least one of the user-selected sub-user identities.

5. A method comprising:

storing, in a database, a profile keyed to a user identity and containing one or more user-selected categories to track transactions associated with said user identity, wherein individual user-selected categories include a user pre-set limit; and

causing communication, over a communication medium and to a receiving device, of transaction summary data in the database for at least one of the one or more user-selected categories, said transaction summary data containing said at least one user-selected category's user pre-set limit.

6. The method of claim 5, wherein the individual user-selected categories further include one or more purchasable items.

7. The method of claim 6 further comprising assigning individual purchasable items to one or both of: a natural category or a user-specified category.

8. The method of claim 5, wherein said at least one user-selected category is associated with one or more user-selected sub-user identities, and wherein said transaction summary data includes one or more sub-user transactions associated with at least one of the user-selected sub-user identities.

9. The method of claim 5, wherein the communication medium comprises, at least in part, a network communication medium.

10. The method of claim 5, wherein the communication medium comprises, at least in part, a wireless communication medium.

11. The method of claim 5, wherein the communication medium comprises, at least in part, a cellular communication medium.

12. A method comprising:

storing, in a database, a profile keyed to a user identity and containing one or more user-selected categories to track transactions associated with said user identity, wherein individual user-selected categories include a user pre-set limit; and

causing communication, over a communication medium and to a receiving device, of transaction summary data in the database for at least one of the one or more user-selected categories, said transaction summary data containing said at least one user-selected category's user pre-set limit, and wherein said transaction summary data is configured to be presented by the receiving device in a table.

13. The method of claim 12, wherein the individual user-selected categories further include one or more purchasable items.

14. The method of claim 13 further comprising assigning individual purchasable items to one or both of: a natural category or a user-specified category.

15. The method of claim 12, wherein said at least one user-selected category is associated with one or more user-selected sub-user identities, and wherein said transaction summary data includes one or more sub-user transactions associated with at least one of the user-selected sub-user identities.

16. The method of claim 12, wherein the communication medium comprises, at least in part, a network communication medium.

17. The method of claim 12, wherein the communication medium comprises, at least in part, a wireless communication medium.

18. The method of claim 12, wherein the communication medium comprises, at least in part, a cellular communication medium.

19. A system comprising:

means for listing financial transactions for a user which occurred during a last accounting period, said financial transactions listed in accordance with one or more user-selected categories; and

means for presenting, in association with an individual user-selected category, an amount of the financial transactions in said individual user-selected category for said last accounting period together with a user-identified category limit associated with said individual user-selected category.

20. The system of claim 19 further comprising means for presenting a user profile pertaining to the financial transactions, said profile being presented using one or more of the following: the Internet, email, telephone or physically supplied information.

21. The system of claim 19 further comprising:

means for accepting one or more changes to at least one of the one or more user-selected categories, the one or more changes pertaining to anticipated financial transactions; and

means for causing storage of said one or more changes for subsequent use.

22. The system of claim 19 further comprising means for listing, in association with at least one of the one or more user-selected categories, one or more sub users and their respective authorized amounts.

23. The system of claim 19 further comprising means for listing, in association with at least one of the one or more user-selected categories, one or more sub users and their respective times of usage.

24. The system of claim 19 further comprising means for allowing a user to change a natural association of items within at least one of the one or more user-selected categories.

* * * * *

US007757298B2

(12) United States Patent

Shuster

(10) Patent No.: **US 7,757,298 B2**

(45) Date of Patent: ***Jul. 13, 2010**

(54) **METHOD AND APPARATUS FOR IDENTIFYING AND CHARACTERIZING ERRANT ELECTRONIC FILES**

(76) Inventor: **Gary Stephen Shuster**, 2067 Manzanita Dr., Oakland, CA (US) 94611

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1383 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/145,125**

(22) Filed: **Jun. 3, 2005**

(65) **Prior Publication Data**

US 2005/0228795 A1 Oct. 13, 2005

Related U.S. Application Data

(63) Continuation of application No. 09/561,751, filed on Apr. 29, 2000, now Pat. No. 6,922,781.

(60) Provisional application No. 60/132,093, filed on Apr. 30, 1999, provisional application No. 60/142,332, filed on Jul. 3, 1999, provisional application No. 60/157,195, filed on Sep. 30, 1999.

(51) **Int. Cl.**

G06F 7/04 (2006.01)

(52) **U.S. Cl.** **726/30**; 726/26; 713/165

(58) **Field of Classification Search** 726/22, 726/26, 30; 713/189, 165, 188

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,864,616	A	*	9/1989	Pond et al.	713/165
5,519,865	A	*	5/1996	Kondo et al.	707/1
5,530,757	A	*	6/1996	Krawczyk	713/188
5,809,138	A		9/1998	Netiv	
5,832,208	A		11/1998	Chen et al.	
5,835,722	A	*	11/1998	Bradshaw et al.	709/225
5,905,800	A		5/1999	Moskowitz et al.	
5,978,791	A	*	11/1999	Farber et al.	707/2
5,983,351	A	*	11/1999	Glogau	726/26
5,996,113	A	*	11/1999	Korn et al.	714/807

(Continued)

FOREIGN PATENT DOCUMENTS

WO	WO9825373	*	6/1998

(Continued)

OTHER PUBLICATIONS

Kalker et al, "Music2Share—Copyright-Compliant Music Sharing in P2P Systems", IEEE, Jun. 2004, p. 961-960.*

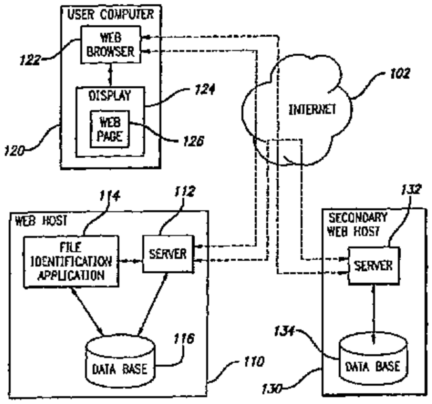
Primary Examiner—Ponnoreay Pich

(74) *Attorney, Agent, or Firm*—Knobbe Martens Olson & Bear, LLP

(57) **ABSTRACT**

A computer system includes a, server having a memory connected thereto. The server is adapted to be connected to a network to permit remote storage and retrieval of data files from the memory. A file identification application is operative with the server to identify errant files stored in the memory. The file identification application provides the functions of: (1) selecting a file stored in said memory; (2) generating a unique checksum corresponding to the stored file; (3) comparing said unique checksum to each of a plurality of previously generated checksums, wherein the plurality of previously generated checksums correspond to known errant files; and (4) marking the file for deletion from the memory if the unique checksum matches one of the plurality of previously generated checksums.

16 Claims, 6 Drawing Sheets



U.S. PATENT DOCUMENTS

6,081,897	A	*	6/2000	Bersson	726/32
6,182,081	B1	*	1/2001	Dietl et al.	707/102
6,209,097	B1	*	3/2001	Nakayama et al.	713/193
6,236,768	B1	*	5/2001	Rhodes et al.	382/306
6,289,341	B1	*	9/2001	Barney	707/6
6,510,513	B1	*	1/2003	Danieli	713/156
6,530,022	B1	*	3/2003	Blair et al.	713/186
6,577,920	B1		6/2003	Hypponen et al.	
6,643,696	B2		11/2003	Davis et al.	
6,922,781	B1		7/2005	Shuster	
7,120,274	B2	*	10/2006	Kacker et al.	382/100
2002/0087885	A1	*	7/2002	Peled et al.	713/201
2005/0108248	A1	*	5/2005	Natunen	707/10

FOREIGN PATENT DOCUMENTS

WO	WO9842098	*	9/1998

* cited by examiner

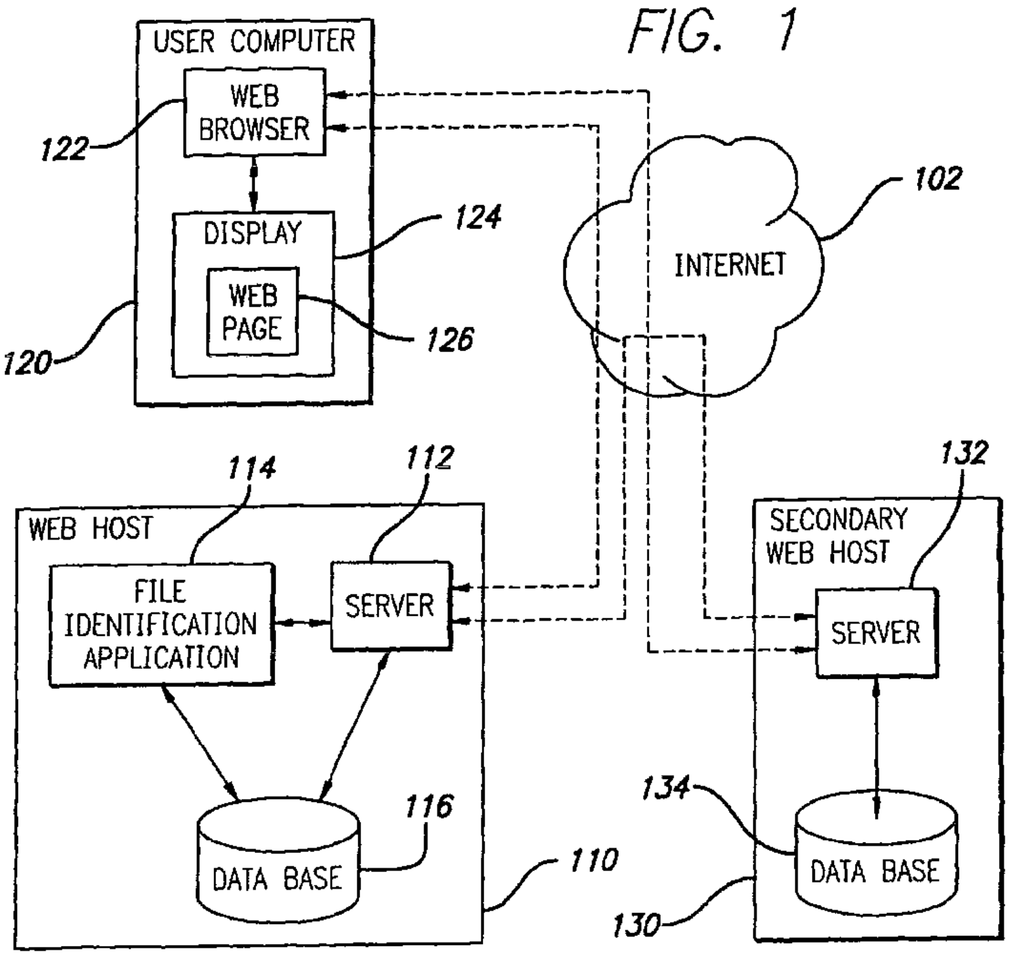

USER COMPUTER
WEB BROWSER
DISPLAY
WEB PAGE
122
124
126
120
INTERNET
102
WEB HOST
FILE IDENTIFICATION APPLICATION
SERVER
DATA BASE
114
112
116
110
SECONDARY WEB HOST
SERVER
DATA BASE
132
134
130

FIG. 1

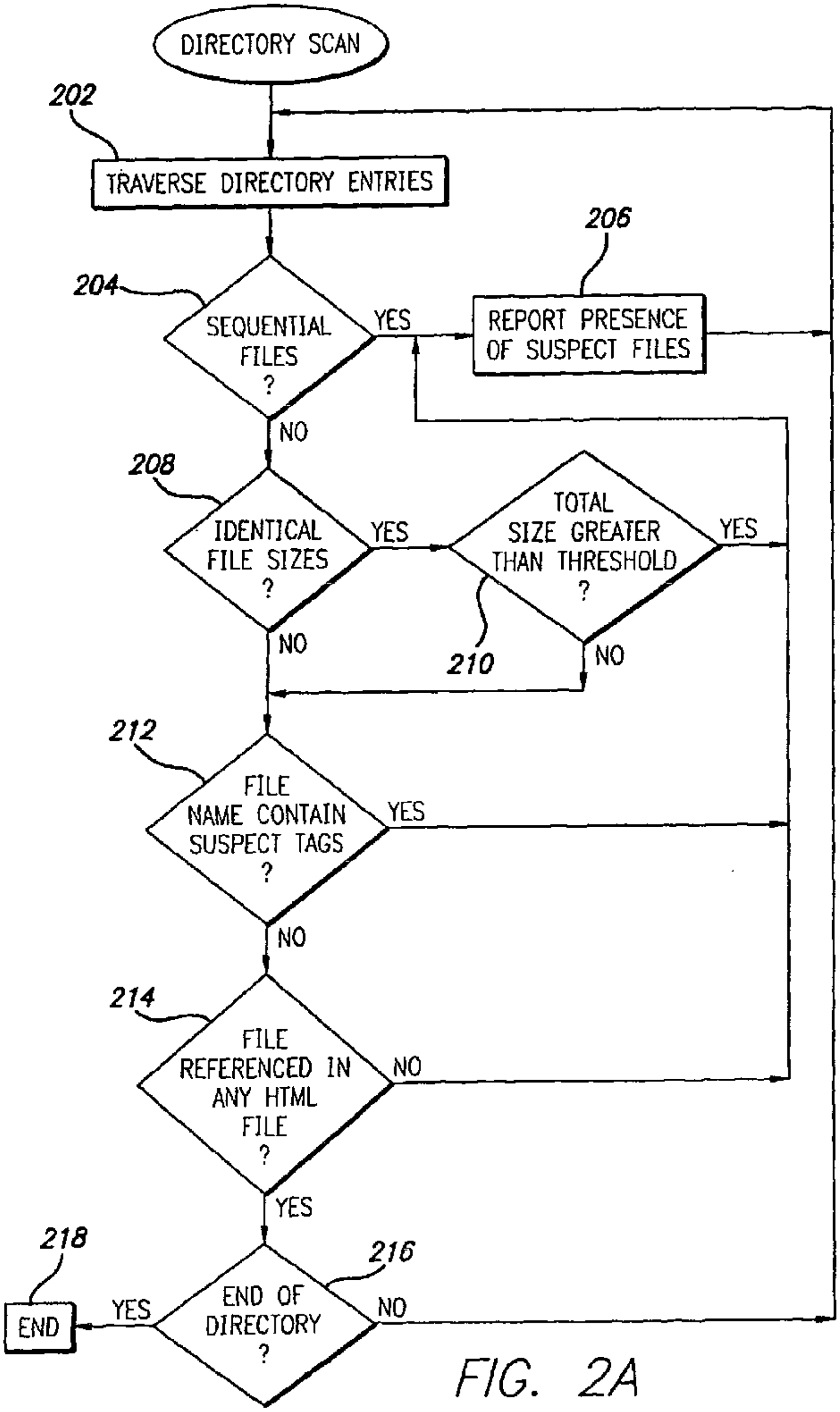

DIRECTORY SCAN
202
TRAVERSE DIRECTORY ENTRIES
204
SEQUENTIAL FILES ?
YES
206
REPORT PRESENCE OF SUSPECT FILES
NO
208
IDENTICAL FILE SIZES ?
YES
TOTAL SIZE GREATER THAN THRESHOLD ?
YES
NO
210
NO
212
FILE NAME CONTAIN SUSPECT TAGS ?
YES
NO
214
FILE REFERENCED IN ANY HTML FILE ?
NO
YES
218
216
END OF DIRECTORY ?
YES
NO
END

FIG. 2A

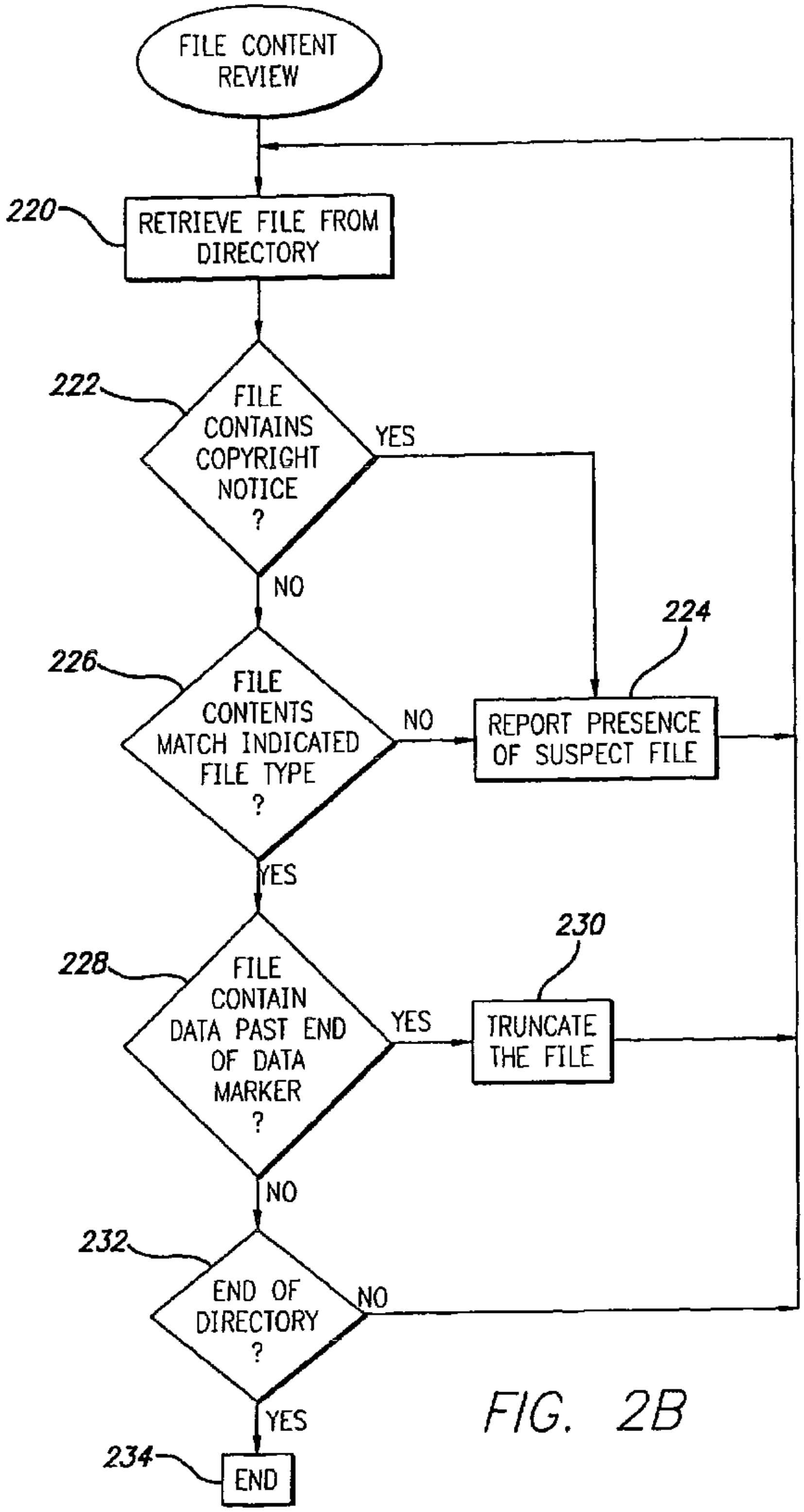

FILE CONTENT REVIEW
220
RETRIEVE FILE FROM DIRECTORY
222
FILE CONTAINS COPYRIGHT NOTICE ?
YES
NO
224
REPORT PRESENCE OF SUSPECT FILE
226
FILE CONTENTS MATCH INDICATED FILE TYPE ?
NO
YES
228
FILE CONTAIN DATA PAST END OF DATA MARKER ?
YES
230
TRUNCATE THE FILE
NO
232
END OF DIRECTORY ?
NO
YES
234
END

FIG. 2B

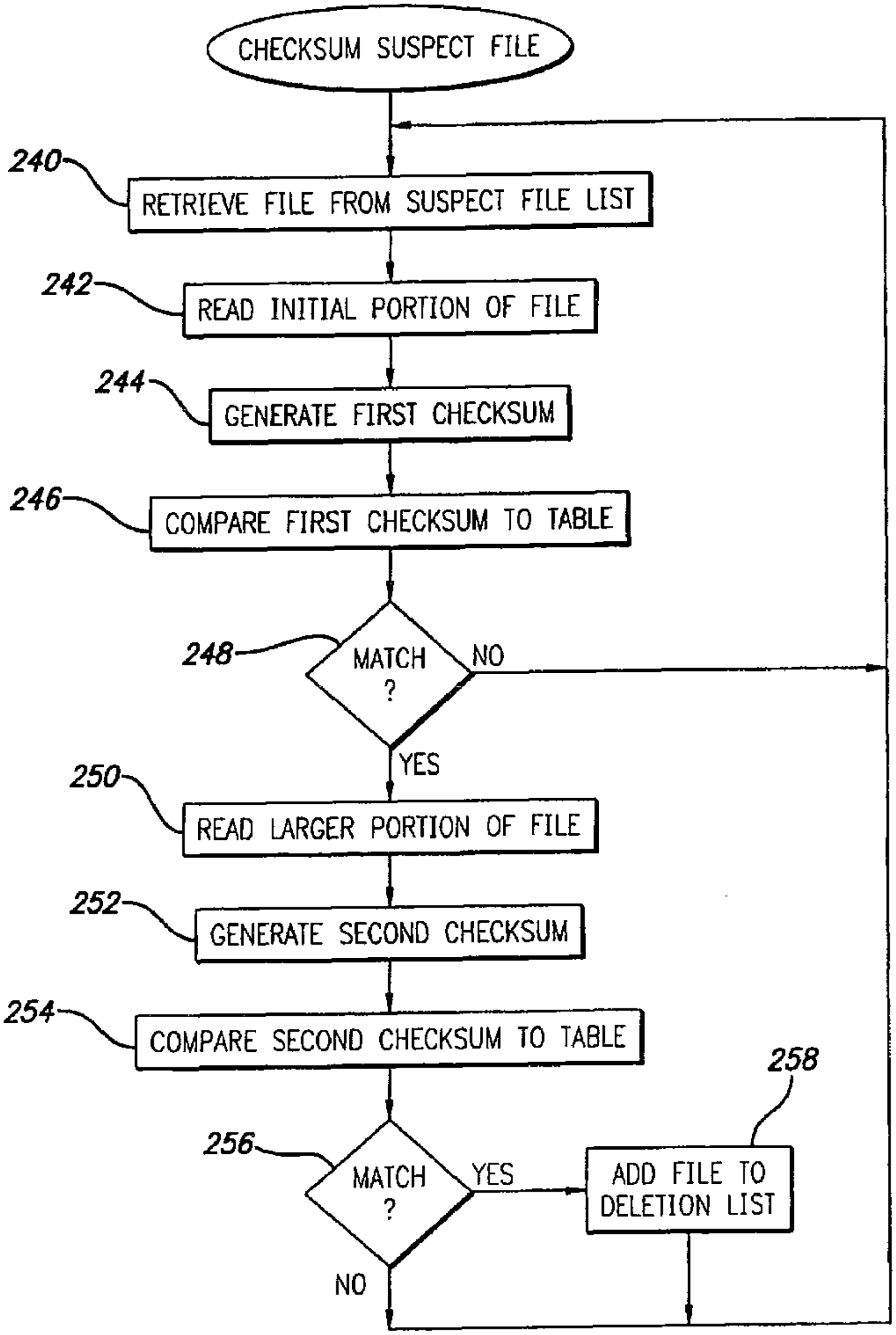

CHECKSUM SUSPECT FILE
240
RETRIEVE FILE FROM SUSPECT FILE LIST
242
READ INITIAL PORTION OF FILE
244
GENERATE FIRST CHECKSUM
246
COMPARE FIRST CHECKSUM TO TABLE
248
MATCH ?
NO
YES
250
READ LARGER PORTION OF FILE
252
GENERATE SECOND CHECKSUM
254
COMPARE SECOND CHECKSUM TO TABLE
258
256
MATCH ?
YES
ADD FILE TO DELETION LIST
NO

FIG. 2C

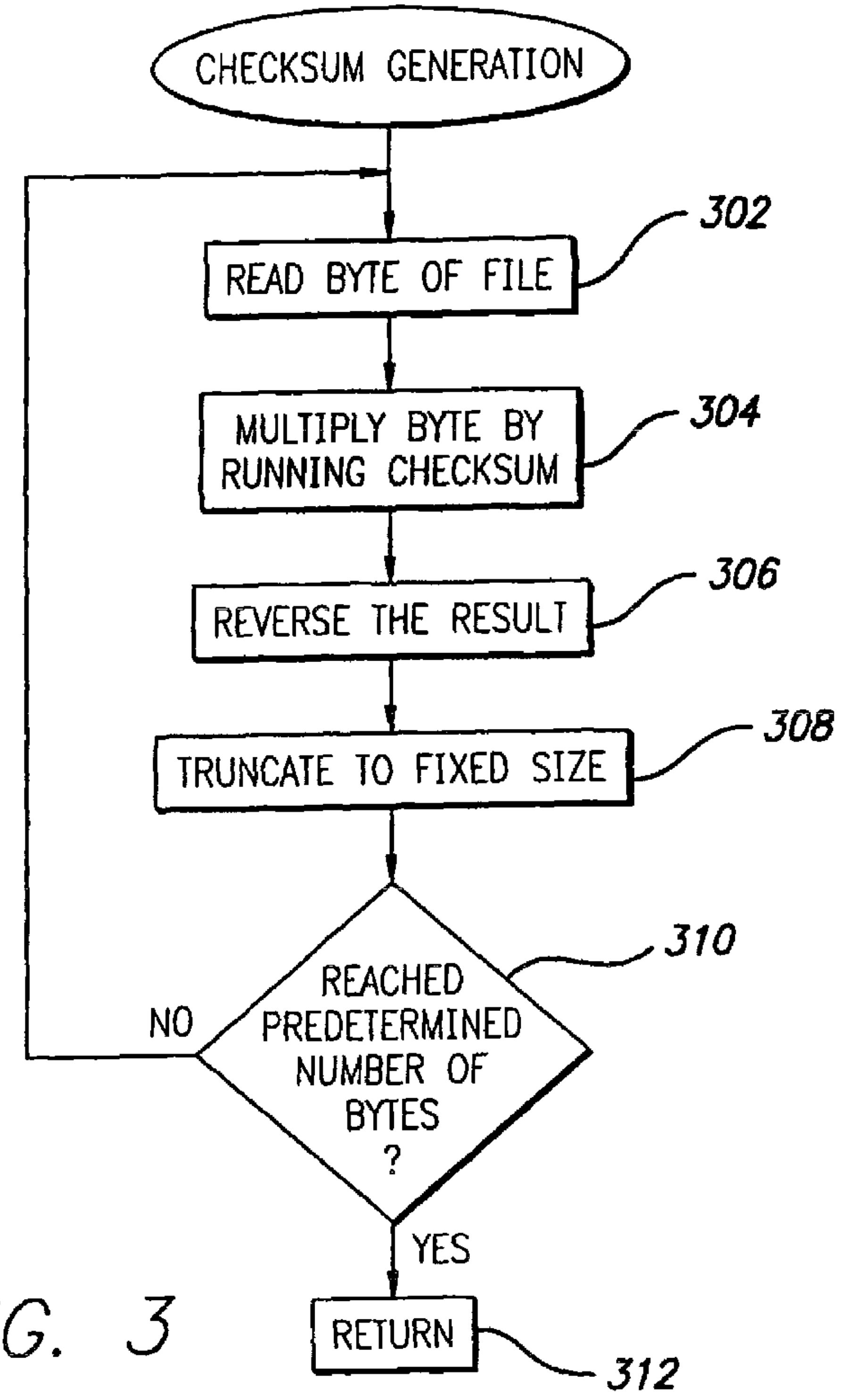

CHECKSUM GENERATION
READ BYTE OF FILE
302
MULTIPLY BYTE BY RUNNING CHECKSUM
304
REVERSE THE RESULT
306
TRUNCATE TO FIXED SIZE
308
REACHED PREDETERMINED NUMBER OF BYTES ?
310
NO
YES
RETURN
312

FIG. 3

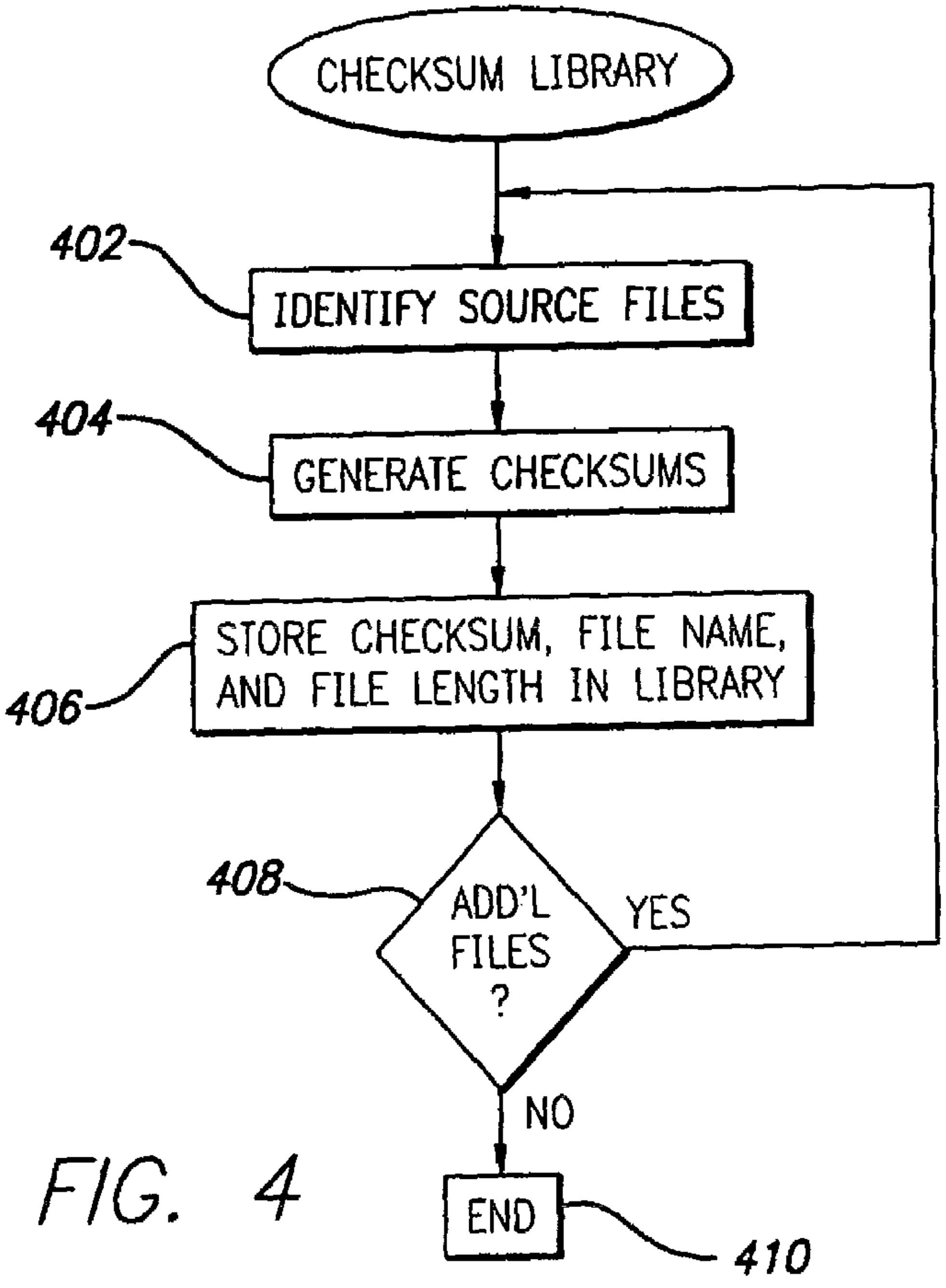

CHECKSUM LIBRARY
402
IDENTIFY SOURCE FILES
404
GENERATE CHECKSUMS
406
STORE CHECKSUM, FILE NAME, AND FILE LENGTH IN LIBRARY
408
ADD'L FILES ?
YES
NO
END
410

FIG. 4

METHOD AND APPARATUS FOR IDENTIFYING AND CHARACTERIZING ERRANT ELECTRONIC FILES

RELATED APPLICATIONS

This application is a continuation of application Ser. No. 09/561,751 filed Apr. 29, 2000, now U.S. Pat. No. 6,922,781, which claims priority pursuant to 35 U.S.C. §119(e) to U.S. Provisional Application Nos. 60/132,093, filed Apr. 30, 1999; 60/142,332, filed Jul. 3, 1999; and 60/157,195, filed Sep. 30, 1999. All of the foregoing non-provisional and provisional applications are specifically incorporated by reference herein, in their entirety.

COPYRIGHT NOTICE

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to electronic files stored on computers, and more particularly, to methods and apparatus for identifying and characterizing errant electronic files stored on computer storage devices.

2. Description of Related Art

The use of public and shared computing environments has proliferated due to the popularity of the Internet. Many Internet service providers (ISP) offer Web hosting services at low or no cost in which registered users can place their own Web sites on the ISP's servers. These individual Web sites allow users to store and access electronic files that are uploaded to the servers. As a result of this proliferation, the administration of the large number of stored electronic files has become an important aspect of such Web hosting services. In view of the relative ease of public access to these electronic file storage resources, there is also widespread abuse of Web server space in which users upload files that are offensive, illegal, unauthorized, or otherwise undesirable and thus wasteful of storage resources. These file types are predominantly of four types: music, video, software and graphics. Many such files may contain pornography in violation of the terms of use of the Web hosting service. Moreover, the copying of these files to the Web server may be in violation of U.S. copyright laws. Consequently, the identification and removal of such files represents a significant administrative burden to the Web hosting services. In addition, the presence of certain files (such as depictions of child pornography or copyrighted music files) on user computers on corporate networks poses great legal risks to the corporation.

Such files can be selected for review and characterized as acceptable or unacceptable to the system administrator using an automated or manual process. Unfortunately, many undesirable files are not easily recognizable and cannot be detected and characterized. A manual review of the content of the files stored on the storage resource is usually not economically feasible, and is also not entirely effective at identifying undesirable files. Illicit users of Web hosting services have devised numerous techniques for disguising improper files wherein even easily recognizable file types are disguised as less recognizable file types. One such technique for disguising files is to split them into parts so that (i) they cannot be detected by simple searches for large files, and (ii) they can be downloaded or uploaded in smaller chunks so that if a transfer is interrupted, the entire download or upload is not lost. The split files may also be renamed so as to hide their true file type. For example, a search for oversized music files (*.mp3) would not turn up a huge file named "song.txt" because it appears to the system as a text file.

Another technique for hiding files is to append them to files that legitimately belong on a web server. By way of example, a Web site may be created called "Jane's Dog's Home Page." Jane gets ten small pictures of her dog, converts them to a computer readable format (for example, jpeg) and saves them on her computer. She then splits stolen, copyrighted software into ten parts. She appends each part to the end of one of the jpeg files. She then uploads these to a web server. Upon a manual review of the web page, the administrator of the site would not notice that the otherwise innocuous dog pictures actually contain stolen software, because each of the files would in fact display a photo of a dog. Thus, even if the files were reported for manual review by software doing a simple search for oversized files, the files would be left on the server because they appear to be legitimate. While these files can sometimes be identified by name or size alone, these methods lead to unacceptable numbers of false positives and false negatives as file sizes and names are changed.

Free and low cost web hosting services typically rely on advertising revenue to fund their operation. An additional abuse of these web hosting services is that they can be circumvented such that the advertisements are not displayed. Typically, the advertising content is displayed on text or hypertext pages. If a user stores graphics or other non-text files on a free web hosting server, yet creates a web page elsewhere on a different service that references these graphics or non-text files, the free web hosting service pays the storage and bandwidth costs for these files without deriving the revenue from advertisement displays.

A need exists, therefore, to provide a method and apparatus for identifying and characterizing errant electronic files stored on computer storage devices, that makes use of a variety of file attributes to reliably characterize files according to pre-set criteria, that is not easily circumvented, and that reduces the amount of manual review necessary to verify proper operation.

SUMMARY OF THE INVENTION

In accordance with the teachings of the present invention, a method and apparatus are provided for identifying and characterizing files electronically stored on a computer storage device. More particularly, an embodiment of the invention further comprises a computer system that includes a server having a memory connected thereto. The server is adapted to be connected to a network to permit remote storage and retrieval of data files from the memory. A file identification application is operative with the server to identify errant files stored in the memory. The file identification application provides the functions of: (1) selecting a file stored in said memory; (2) generating a unique checksum corresponding to the stored file; (3) comparing said unique checksum to each of a plurality of previously generated checksums, wherein the plurality of previously generated checksums correspond to known errant files; and (4) marking the file for deletion from the memory if the unique checksum matches one of the plurality of previously generated checksums.

A more complete understanding of the method and apparatus will be afforded to those skilled in the art, as well as a realization of additional advantages and objects thereof, by a consideration of the following detailed description of the preferred embodiment. Reference will be made to the appended sheets of drawings that will first be described briefly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a wide area network in which a web host delivers information in the form of web pages to users;

FIG. 2A is a flow chart illustrating a method of scanning a file directory to identify suspect files stored in a database in accordance with an embodiment of the invention;

FIG. 2B is a flow chart illustrating a method of reviewing file contents to identify suspect files;

FIG. 2C is a flow chart illustrating a method of checksumming the suspect files;

FIG. 3 is a flow chart illustrating a method of generating checksum values; and

FIG. 4 is a flow chart illustrating a method of generating a checksum library.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention satisfies the need for a method and apparatus for identifying and characterizing errant electronic files stored on computer storage devices, that makes use of a variety of file attributes to reliably characterize files according to pre-set criteria, that is not easily circumvented, and that reduces the amount of manual review necessary to verify proper operation. In the detailed description that follows, like element numerals are used to describe like elements illustrated in one or more of the figures.

Referring first to FIG. 1, a block diagram is illustrated of a wide area network in which information is delivered to users in the form of web pages. It is anticipated that the present system operates with a plurality of computers that are coupled together on a communications network, such as the Internet or a wide area network. FIG. 1 depicts a network that includes a user computer 120 that communicates with a Web host 110 though communication links that include the Internet 102. The user computer 120 may be any type of computing device that allows a user to interactively browse websites, such as a personal computer (PC) that includes a Web browser application 122 executing thereon (e.g., Microsoft Internet Explorer™ or Netscape Communicator™). The Web host 110 includes a server 112 that can selectively deliver graphical data files in the form of HyperText Markup Language (HTML) documents to the user computer 120 using the HyperText Transport Protocol (HTTP). Currently, HTML 2.0 is the standard used for generating Web documents, though it should be appreciated that other coding conventions could also be used within the scope of the present invention. The server 112 accesses HTML documents stored within a database 116 that can be requested, retrieved and viewed at the user computer via operation of the Web browser 122. The database 116 may also contain many other types of files, including text, graphics, music, and software files. It should be appreciated that many different user computers may be communicating with the server 112 at the same time.

As generally known in the art, a user identifies a Web page that is desired to be viewed at the user computer 120 by communicating an HTTP request from the browser application 122. The HTTP request includes the Uniform Resource Locator (URL) of the desired Web page, which may correspond to an HTML document stored on the database 116 of the Web host 110. The HTTP request is routed to the server 112 via the Internet 102. The server 112 then retrieves the HTML document identified by the URL, and communicates the HTML document across the Internet 102 to the browser application 122. The HTML document may be communicated in the form of plural message packets as defined by standard protocols, such as the Transport Control Protocol/Internet Protocol (TCP/IP). A user may also download any other type of file from the database 116 in the same manner.

FIG. 1 further illustrates a secondary Web host 130 having a server 132 and database 134 similar to that of the primary Web host 110. The user computer 120 can communicate with the secondary Web host 130 in the same manner as described above. Moreover, the primary Web host 110 can communicate with the secondary Web host 130 in the same manner. The pertinence of this communication path will become more clear from the following description of the present method. The Web host 110 further comprises a file identification application 114 that analyzes the data files stored on the database 116 in order to identify errant files in accordance with the present invention. The file identification application 114 may comprise a program executing on the same computer as the server 112, or may be executing on a separate computer. The file identification application tests various attributes of the files stored on the database to determine whether they satisfy a particular profile that corresponds to an errant file. Source code for a preferred embodiment of a file identification application is attached hereto as an exhibit.

A widely accepted characteristic of the Internet is that files are copied relentlessly and without permission. This is particularly true of illicit files, such as adult content, pornographic material or illegally copied software, music or graphics. Thus, a photograph showing up on a single Web site may be propagated to hundreds of other Web sites within days. Although the file name is often changed, and transmission errors often result in premature truncation of the file (and thus a new file length), the initial portion of the file remains identical as it is propagated throughout the Internet. Another characteristic of the Internet is that illicit files, such as music, video and software, all have one common attribute—they are very large once reassembled. It is therefore necessary to (i) identify oversized files that have been uploaded in parts, and (ii) identify "hidden" files that are appended to otherwise legitimate files. As will be further described below, an aspect of the present invention takes advantage of these characteristics of the Internet.

Referring now to FIGS. 2A-2C, a method for identifying and characterizing files is illustrated in accordance with an embodiment of the invention. The method would be executed by the file identification application 114 described above with respect to FIG. 1. FIG. 2A illustrates an exemplary method of scanning a file directory to identify suspect files stored in a database. Suspect files are ones that are suspected of being improper, and are marked for further testing. The database 116 includes a directory that identifies the files stored therein based on various attributes, including file name and file size. It will be appreciated from the following discussion that the method of FIGS. 2A-2C relates specifically to the identification of pornographic materials in view of the particular selection criteria that is utilized; however, it will be understood to persons of ordinary skill in the art that the selection criteria can be modified to identify other types of illicit files. Starting at step 202, the application traverses the directory in order to analyze the numerous directory entries. The application may construct a relational database of the directory entries in order to sort on the various fields of the directory. This step may be performed repeatedly as a continuing process through this identifying process, and would have to be repeated periodically to identify new files that are added to the database **116**.

At step **204**, the application determines whether there are any sequentially numbered files within the directory. Sequential files can be identified by analyzing and comparing the file names to each other. One attribute of pornographic materials is that they are often uploaded to a server as part of a series of photographs. Thus, the file names may include an embedded numerical designation such as "xxx001.jpg" or "xxx002.jpg". The user may define at what level of folders the software will look for sequentially numbered, lettered, or otherwise identified files. For example, if a file server is divided into folders lettered from "AA" to "ZZ", and each folder contains Web sites with names in which the first two letters correspond to the name of the file folder, the user could decide to treat all folders on the server as a single Web site, or to treat only Web sites within the same folder as a single Web site, or to treat each Web site individually. In the preferred embodiment, each Web site is considered on its own without reference to other Web sites, although the invention need not be limited in this manner.

If any such sequential files are identified, they are reported as suspect files at step **206**. Then, the application returns to step **202** and continues traversing through the directory entries. If no sequential files are identified at step **204**, the application next determines at step **208** whether there are any files having identical file sizes. Another attribute of stolen intellectual property materials such as music files is that they are often broken up into several pieces in order to thwart their detection by simple searches for large files, and also to enable them to be downloaded or uploaded in smaller chunks to facilitate transfer. The presence of two or more files having identical file size within the, directory is an indicator that they may be pieces of a single, larger, illicit file. If there are plural files with identical file sizes, the application determines at step **210** whether the total size of the identical files summed together would exceed a predetermined threshold. As noted above, illicit files tend to be unusually large, so the predetermined threshold would be selected to correspond with the largest size of a typical non-illicit file. If the total size does exceed the predetermined threshold, then the identical files are reported as suspect files at step **206**.

More particularly, the application may manipulate the file names to determine whether they are in fact likely to be parts of a single, larger file. An alternative way to determine whether files should be aggregated is to delete all numbers from the file names. Any files that are identically named after the elimination of all numbers would be marked as potentially responsive and their names and aggregate size would be reported. Of course, this can be limited to numbers in conjunction with specified letters (such as r00, r41, etc., as the "r" denotation often indicates file compression and division via the RAR method). Similarly, this can be limited to specified file types (whether identified by the file type suffix to the file name, or by examination of the actual contents of the file) or files other than specified types (for example, legitimate graphics files such as *.jpg are often sequentially numbered and may be a good candidate for exclusion). Next, using the original list of file names, any files are identified that differ only by a user-defined number of characters. Such files would be marked as potentially responsive and their names and aggregate size would be reported. Both of the foregoing methods can be set to either ignore the file suffix or file type information or to utilize it. Next, using the original list of file names and sizes, files that are of the same size (or within a user-defined number of bytes of being of the same size) are identified. Any such files are marked as potentially responsive and their names and aggregate size would be reported.

If no identical files are identified at step **208**, or if the total size does not exceed the predetermined threshold at step **210**, the application proceeds to step **212** where it is determined whether the file names contain any suspect tags. An example of a suspect tag is "xxx" which is often used in association with pornographic materials. Another example of a suspect tag is "crc", which refers to a cyclical redundancy check (CRC), i.e., a known error checking technique used to ensure the accuracy of transmitting digital data. When a large file has been broken up into plural smaller files, it is common to include a CRC file in order verify the accurate reconstruction of the large file. The presence of a file having a "crc" tag is an indicator that an illicit or illegal file has been uploaded to the server. A table of predetermined suspect tags may be generated and periodically updated to reflect current usage within Internet newsgroups, Web sites and other facilities for trafficking in pornographic or illicit materials. If any file names containing suspect tags are identified, then the associated files are reported as suspect files at step **206**.

If no suspect tags are identified at step **212**, the application proceeds to step **214** where it is determined whether the file is referenced in any HTML file contained within the directory. Ideally, the files stored on the database would each be linked to HTML files contained within the directory. Where a file is not linked to a local HTML file, this is an indicator that a user is storing graphics or other non-text files that are linked to a Web page hosted elsewhere on a different service. As described above, this situation is undesirable since the free web hosting service pays the storage and bandwidth costs for these files without deriving the revenue from advertisement displays. Accordingly, any file names that are not referenced in an HTML file contained within the directory are reported as suspect files at step **206**. Alternatively, every file bearing a file type capable of causing a web browser to generate hypertext links (i.e. *.htm, *.html, *.shtml, etc.) may also be reviewed. The hypertext links may be then compared against a list of illegal links (for example, links to adult-content Web sites). Any file that contains a hypertext link to such a site is reported as suspect. If all files on the directory are properly referenced in HTML files or contain no illegal links, the application determines whether the end of the directory has been reached at step **216**. If the end of the directory is not yet reached, the application returns to step **202** to continue traversing the directory and identifying suspect files. Otherwise, this portion of the application ends at step **218**.

Once a review of the directory entries is complete, the next step is to review the content of the files listed on the directory to see if additional files should be added to the suspect file list. This review may address every file listed on the directory not already listed on the suspect file list, or may be further narrowed using particular selection criteria specific to the type of illicit file, i.e., pornography, copyright infringement, etc. FIG. 2B illustrates an exemplary method of reviewing file contents. At step **220**, the application retrieves a file from the directory. At step **222**, the retrieved file is examined to identify whether the file contains a copyright notice or the symbol ©. The presence of a copyright notice in the file is an indicator that the file has been uploaded to the server unlawfully, and likely contains graphics, text, software or other material that is protected by copyright. Any files containing the copyright notice would be reported as a suspect file and added to the suspect file list at step **224**. This copyright notice check procedure can also be used to ensure compliance with appropriate copyright laws. Alternatively, the file can be simply marked for deletion. The application then returns to step **220** and retrieves the next file.

If the file does not contain a copyright notice, the application passes to step **226**, in which the retrieved file is examined to determine whether the file structure is as expected for a file of the indicated type. For example, the file type "jpg" should contain a header structure with the values "255 216 255 224". Alternatively, files can be checked to ensure that they actually contain the type of data described by the file type marker (i.e., a file named *jpg should contain a jpg image). If the file does not match the indicated file type, the file can be reported as a suspect file and added to the suspect file list at step **224**, or simply marked for deletion. Another alternative approach would be to replace files containing data of a type different than that indicated by their file type marker by a file stating that the original file was corrupted. Yet another approach would be to retype the file (i.e. *jpg can be retyped to *.zip if it contained a zipped file and not a jpg). Further, certain file types can be aggregated. For example, *.gif and *.jpg files may be aggregated as a single file type, and a file bearing a *.jpg type is considered valid if it contains either a gif or a jpg image. This greatly reduces the problem of mistakenly deleting a file that a consumer has innocently misnamed. The application then returns to step **220** and retrieves the next file.

If the file contents do match the indicated file type, the application determines at step **228** whether the file contains data extending past the end of data marker. If this marker appears before the true end of file, then it is likely that the additional data following the end of data marker constitutes a portion of an illicit file. At step **230**, the file is truncated at the end of file marker. The application then returns to step **220** and retrieves the next file. If the file does not contain data past the end of data marker, the application proceeds to step **232** in which it is determined whether the end of the directory has been reached. If there are still additional files in the directory to review, the application returns to step **220** and retrieves the next file. If there are no additional files, the file content review process ends at step **234**.

After the files within the directory have been reviewed and a list of suspect files generated, the next step is to checksum the suspect files and compare the results against a library of checksum values corresponding to known illicit files. The generation of this list of known illicit files will be described below with respect to FIG. **4**. FIG. **2C** illustrates an exemplary method of checksumming the suspect files. A checksum is a unique number based upon a range or ranges of bytes in a file. Unlike checksums as they are traditionally used in the computing field, the checksum described herein is not related to the total number of bytes used to generate the number, thus reducing a traditional problem with checksums, namely that similar file lengths are more likely to generate the same checksum than are dissimilar file lengths. In a preferred embodiment of the invention, two separate checksums are generated for a file corresponding to two different length portions of the file. While it is possible that the first checksum based on a shorter length portion of the file may falsely match the checksum of another file, it is highly unlikely that the second checksum would result in a false match. In addition, the use of an initial checksum based upon a small amount of data, reduces the burden on the network and file server. This reduction is a result of the ability to disqualify a file that does not match the first checksum without the need to read the larger amount of data necessary to generate the second checksum.

More particularly, at step **240**, the application retrieves a file from the database identified on the suspect file list. Then, at step **242**, the application reads a first portion of the suspect file. In an embodiment of the invention, the first portion comprises the first one-thousand (1,024) bytes of the file. A first checksum based on this first portion is generated at step **244**. The first checksum is then compared to a library of known checksum values at step **246**, and at step **248** it is determined whether there is a match between the first checksum and the library. This step provides an initial screen of a file. If there is no match, then the file likely does not correspond to a known illicit file. The file may nevertheless constitute improper or unlawful material, and it may therefore be advisable to manually review the file to evaluate its contents. If the file does contain improper or unlawful material, its checksum may be added to the library of known checksums and the file marked for deletion from the database. Conversely, if the manual review does not reveal the file to be improper or unlawful, or based simply on the negative result of the first checksum comparison, the file is removed from the suspect file list, and the application returns to step **240** to retrieve the next file from the suspect file list.

If there is a match based on the initial screen of the file, the application proceeds to step **250** in which a second portion of the file is read. In an embodiment of the invention, the second portion comprises the first ten-thousand (10,240) bytes of the file. A second checksum based on this second portion is generated at step **252**. The second checksum is then compared to a library of known checksum values at step **254**, and at step **256** it is determined whether there is a match between the second checksum and the library. This step provides a more conclusive determination as to whether the file corresponds to a known improper or unlawful file. If there is a match, the file is marked for deletion (or other treatment) at step **258**, and the application returns to step **240** to retrieve the next suspect file. If there is not a match, the file is removed from the suspect file list, and the application again returns to step **240** to retrieve the next suspect file.

The files that are marked for deletion may be listed along with the pertinent information in a database (either via numerous individual files, an actual database such as SQL Server, or otherwise). This database may be manually reviewed and files that should not be deleted removed from the database. A simple file deletion program may then be run that deletes any file in the database.

As noted above, the first one-thousand bytes and the first ten-thousand bytes are used for the two checksums, respectively. For most applications, the use of the entire file or a larger portion of the file is not necessary and indeed may slow the process; however, there is no reason why the entire file or any other subset of the file could not be used. In an alternative embodiment, the first and last portions of the file are used for checksumming, although premature file truncation then becomes a way to defeat the screen. It is also possible to use other data to improve the quality of the initial screen, such as the length of the file and the file name. Any file matching the initial screen criteria is then checked against one or more checksum tests. Yet another alternative embodiment is to simultaneously generate both the initial screen checksum and the confirmation checksum in a single file read, thereby reducing the number of distinct disk access events. Verification is optional when the initial screen is performed using a checksum, as the checksum denotes a nearly certain match.

In an alternative embodiment of the invention, the present method for identifying and characterizing files can be used to block music piracy on the Internet. Each music CD carries certain identifying data that permits unique identification of that CD. MP3 encoders can be configured to encode this information into the first bytes of each MP3 file. As such, the

MP3 file would carry the signature of the music CD it was created from. This would permit a scan of all files on a server for the signature code of a particular CD. When such a code is found, it can be checked against a database of copyrighted music and any matches marked for deletion and/or review. An alternative embodiment would be to prevent MP3 players from working property unless the unique identifier from a CD is found, and that unique identifier can be checked for validity against a checksum or an Internet database.

There are numerous possible algorithms that may be utilized to generate a checksum, with an exemplary algorithm shown in FIG. **3**. At step **302**, a single byte of the file is read. The byte is then multiplied by the current value of the checksum at step **304**. On the first pass through the algorithm, a value of one is used for the current value of the checksum. Next, at step **306**, the result of the previous step is reversed (e.g., 1234 becomes 4321). At step **308**, the result of the previous step is truncated to a predetermined number of digits (e.g., with the predetermined number of digits being nine, 1,234,567,890 becomes 123,456,789). At step **310**, the algorithm determines whether the predetermined number of bytes has been reached. As described above, checksums are performed using the first one-thousand (1,024) and ten-thousand (10,240) bytes in accordance with a preferred embodiment of the invention. If the predetermined number of bytes has not been reached, the algorithm returns to step **302** and continues with the next byte. Conversely, if the predetermined number of bytes has been reached, the algorithm ends at step **312**. An advantage of this algorithm is that the checksum that is generated is independent of the number of bytes that are utilized. This way, the likelihood of false matches is substantially reduced even though the same number of bytes are used to calculate the checksums.

It should be appreciated to persons having ordinary skill in the art the many other types of algorithms could be utilized to achieve results specific to certain types of files. In an alternative embodiment of the invention, checksums of graphics files may be generated based on vector graphics analysis of the files. The graphics file may be reduced to its vector graphics components. The resulting vector graphics image is then reduced to a checksum representing the vector graphics image. The checksum is then checked against a list of checksums generated in a similar matter against known or suspected inappropriate images.

An alternative method of generating a unique checksum for a graphics file is by dividing an image into quadrants or other blocks and comparing the relationships between the zones into which the image is divided. For example, the relative ratio of red to green, green to blue, and blue to red in each of the zones may be calculated, and then recorded. A file could then be altered in a minor way (such as by altering several bits) without defeating the ability of the software to find the file.

Referring now to FIG. **4**, an exemplary process is illustrated for generating the library of checksum values. At step **402**, a source of known illicit files is identified. This may be performed by manually reviewing files already stored on the database **116** of the Web host **110**, such as the files identified as suspect (see FIGS. **2A-2B**). Alternatively, sources of illicit files outside of the Web host **110** may be sought, such as located on a secondary Web host **130**. Certain Web servers may be assumed to contain files matching the criteria (i.e., a Web host that accepts adult content and runs adult oriented ads over that content will contain nearly entirely adult material). Alternatively, a target newsgroup (e.g., alt.binaries.pictures.erotica.female) can provide a source of illicit files. Once an adequate source of files is identified, checksum values are generated at step **404** in the same manner as described above with respect to FIG. **3**. Then, at step **406**, the checksum is stored in a library along with the file name and file length. Lastly, at step **408**, it is determined whether there are other files associated with the identified source of files that can be checksummed in order to further enlarge the library. As will be further described below, the identification of a single source of illicit material will invariably lead to other sources of material. Thus, the library can be expanded at an exponential rate. The process of FIG. **4** is repeated for each new source of illicit material. If no additional source files can be located, the process terminates at step **410**.

Once a single file is located matching a predefined criteria (i.e., adult content), it is almost certain that other files also matching the same criteria will be found together with or in proximity to the original matching file (e.g., a Web site having one pornographic photograph will likely contain others with it). All files located with the matching file can be automatically checksummed, or can be checksummed after a manual review. Thus, the library of checksums is expanded. In view of the nature and prevalence of illicit material on the Internet, it is also likely that the matching files will also appear on other Web sites, and will thus lead to other files meeting the selection criteria that can themselves be checksummed. The expansion of the checksum library is thus exponential, and nearly the entire body of illicit materials on the Internet can be checksummed in this manner. This checksum amplification method in the automated checksumming modality can be further refined by requiring that any given checksummed file appear together with a minimum number of other checksummed files on a minimum number of Web sites before the file represented by the checksum is considered to match the selection criteria.

It should be appreciated that one cannot defeat the present invention by simply altering an illicit image file. Although the alteration of an image file may prevent it from matching an existing checksum, the altered image will invariably be copied and posted on a new Web site together with unaltered, checksummed images, and will be inevitably checksummed using the foregoing process. Furthermore, the process can be modified so as to allow automated checksumming with a greatly reduced risk of the generation of checksums for files that do not match the selection criteria. One approach is to set a file size floor and ceiling and/or file type limitation. Another approach is to create and maintain a list of excluded files, including all publicly available "clip art" and popular mainstream advertising banners, as well as files that show up frequently on legitimate Web sites. Yet another alternative approach is to require an image to appear in proximity to known illicit files, such as files that match existing checksums, a minimum number of times before being added to the checksum library.

Furthermore, certain graphics are quite common in certain types of Web sites. For example, pornographic Web sites almost always contain a "banner" advertising membership in a commercial pornography Web site. There is a very limited universe of such banners. By generating checksums for all available pornographic banners, it is possible to locate nearly all pornographic web sites. Using the checksum amplification method described above, these advertising banner checksums would quickly lead to a very comprehensive catalog of pornographic material checksums. Similarly, illegally copied software sites often have "warez" banners. Other target file types have banners and common graphics associated with them as well.

Files matching the selection criteria can also be located by searching for hyperlinks to checksummed files or to sites known to contain inappropriate material. Thus, whenever a checksum is matched, the URL of the material located is recorded. Any HTML page that links to that material is then identified as likely containing material matching the selection criteria. All other graphics referenced by that HTML page and/or in the same Web site may then be automatically checksummed or flagged for manual review and checksumming.

Certain key words may also be searched for on a Web site. Thus, for example, the word "fuck" in close association with "lolita" should flag a site as likely to contain child pornography. This method is better used in conjunction with a manual review so as to avoid checksumming files that do not match the selection criteria, although it can also be used as an enhancement to the checksum amplification method to confirm that checksums should be automatically generated.

The results of these searches can be returned in a regular text file. Alternatively, the results may be returned in a formatted HTML file that interconnects with the file management system. The HTML file should display a copy of all files on a given Web site matching the checksum(s), all user information as well as other sites using the same password, with the same user name, with the same IP address, or the same e-mail address, and the options to delete the site(s), modify the records, delete the materials, etc. Furthermore, for those file types that cannot be graphically displayed by a Web browser, the "server" modality (see code attached as Exhibit) should be used to return a "file present" or "file absent" graphic to indicate whether the file is present or absent.

In an alternative embodiment of the invention, the present method for identifying and characterizing files may be implemented in a real-time manner to review files as they are uploaded to the Web server. In yet another embodiment of the invention, the present method for identifying and characterizing files may be used to check the contents of desktop computers within a business. Thus, for example, with file and access permissions set correctly, the software could determine whether pornography, child pornography, copyrighted software, or other problematic materials exist on the computers used by employees. Appropriate reporting could then be accomplished. This can also be accomplished by running the software in a standalone package on desktop computers (by parents, for example). For file systems that require locally running software, the software can also be combined with necessary software (for example, the detection software could also serve as the e-mail program for the user, or as the mechanism whereby the user logs into their main server).

An important advantage of the use of checksums to identify and characterize illicit files is that the customer service employees of a Web hosting company can determine with certainty that a file contains illegal contents without actually viewing the file. This is particularly important in retaining employees, as many individuals can become uncomfortable or disturbed by having to view illicit, violent or illegal images. For example, by having a library of child pornography checksums, the computer can simply report "child porn found", and no employee need ever see the image. The customer service employees can then load the illegal file onto a disk to deliver to law enforcement, and terminate the customer account. Another advantage of using the checksums is that it eliminates the need for the Web hosting company to maintain copies of illegal or contraband files in order to verify that files match them. Thus, it is unnecessary to keep a copy of an illegal picture or stolen music file in order to check whether files found on the server match the illicit files.

Lastly, the present method for identifying and characterizing files could be used to provide automatic notification to Web host customers and other interested parties. Any time a file is reported as illegal, a database containing a list of customer data may be accessed to obtain the e-mail address of the site operator. An automated e-mail message may be generated (optionally copied to the Web hosting company's staff) indicating that the site has been marked for review and/or deletion. Alternatively, the fax number of the customer may be accessed and the same message sent via fax. Alternatively, the phone number may be accessed and a text-to-voice system used to send an automated telephone message. Alternatively, postal mail may be printed with the customer's address and the same message.

Having thus described a preferred embodiment of a method and apparatus for identifying and characterizing errant electronic files, it should be apparent to those skilled in the art that certain advantages have been achieved. It should also be appreciated that various modifications, adaptations, and alternative embodiments thereof may be made within the scope and spirit of the present invention. The invention is further defined by the following claims.

What is claimed is:

1. A computer-implemented method for identifying and characterizing stored electronic files, said method comprising:

under control of one or more configured computer systems:

selecting a file from a plurality of files stored in a computer storage medium, wherein selecting the file is performed according to at least one of:

selecting the file based on the size of the file by determining whether an aggregate size of plural identically-sized files exceeds a predetermined threshold;

selecting the file based on whether content of the file matches a file type indicated by a name of the file; or

selecting the file based on whether the file comprises data beyond an end of data marker for the file;

generating an identification value associated with the selected file, wherein the identification value is representative of at least a portion of the content of the selected file;

comparing the generated identification value to one or more identification values associated with one or more of a plurality of unauthorized files; and

characterizing the file as an unauthorized file if the identification value matches one of the plurality of identification values associated with the unauthorized files.

2. The computer-implemented method of claim **1**, further comprising selecting the file from one of a plurality of sequentially-ordered files in a directory of the computer storage medium.

3. The computer-implemented method of claim **1**, wherein generating an identification value comprises generating a checksum.

4. The computer-implemented method of claim **3**, wherein-generating an identification value comprises generating a first checksum corresponding to a first portion of said stored file and a second checksum corresponding to a second portion of said stored file.

5. The computer-implemented method of claim **3**, wherein generating an identification value comprises generating a first checksum corresponding to a first portion of said stored file and a second checksum corresponding to a larger portion of said stored file that includes the first portion.

6. The computer-implemented method of claim **1**, further comprising processing a plurality of known unauthorized files to generate the plurality of identification values.

7. The computer-implemented method of claim **1**, further comprising presenting the identified unauthorized file for human review prior to disposing of it.

8. The computer-implemented method of claim 1, further comprising automatically notifying a third party that the file has been identified.

9. The computer-implemented method of claim 1, further comprising deleting the identified unauthorized file from the computer storage medium.

10. A computer system, comprising:

a server having a memory connected, thereto, said server being adapted to be connected to a network to permit remote storage and retrieval of data files from the memory; and

a file identification application operative with the server to identify unauthorized files stored in the memory, the file identification application providing the functions of:

selecting a file from a plurality of files stored in the memory, wherein selecting the file is performed according to at least one of:

selecting the file by determining whether an aggregate size of plural identically-sized files exceeds a predetermined threshold;

selecting the file based on whether content of the file matches a file type indicated by a name of the file; or

selecting the file based on whether the file comprises data beyond an end of data marker for the file;

generating an identification value associated with the selected file, wherein the identification value is representative of at least a portion of the content of the selected file;

comparing the generated identification value to one or more identification values associated with one or more of a plurality of unauthorized files; and

characterizing the file as an unauthorized file if the identification value matches one of the plurality of identification values associated with the unauthorized files.

11. The system of claim 10, wherein the application further comprises the function of selecting the file from one of a plurality of sequentially-ordered files in a directory of the computer storage medium.

12. The system of claim 10, wherein the application further comprises the function of selecting the file from a plurality of files stored in the computer storage medium, based on size of the file.

13. The system of claim 10, wherein generating an identification value comprises generating a checksum.

14. The system of claim 13, wherein generating an identification value comprises generating a checksum corresponding to a first portion of the selected file and a second checksum corresponding to a second portion of the selected file.

15. The system of claim 13, wherein generating an identification value comprises generating a first checksum corresponding to a first portion of the selected file and a second checksum corresponding to a larger portion of the selected file that includes the first portion.

16. A non-transitory computer-readable storage medium having instructions stored thereon that, in response to execution by a computing device, cause the computing device to perform a operations comprising:

selecting a file from a plurality of files stored in a computer storage medium, wherein selecting the file is performed according to at least one of:

selecting the file based on the size of the file by determining whether an aggregate size of plural identically-sized files exceeds a predetermined threshold;

selecting the file based on whether content of the file matches a file type indicated by a name of the file; or

selecting the file based upon whether the file comprises data beyond an end of data marker for the file;

categorizing the selected file as an unauthorized file based on a comparison of an identification value associated with the selected file with one or more identification values associated with one or more of a plurality of unauthorized files.

* * * * *